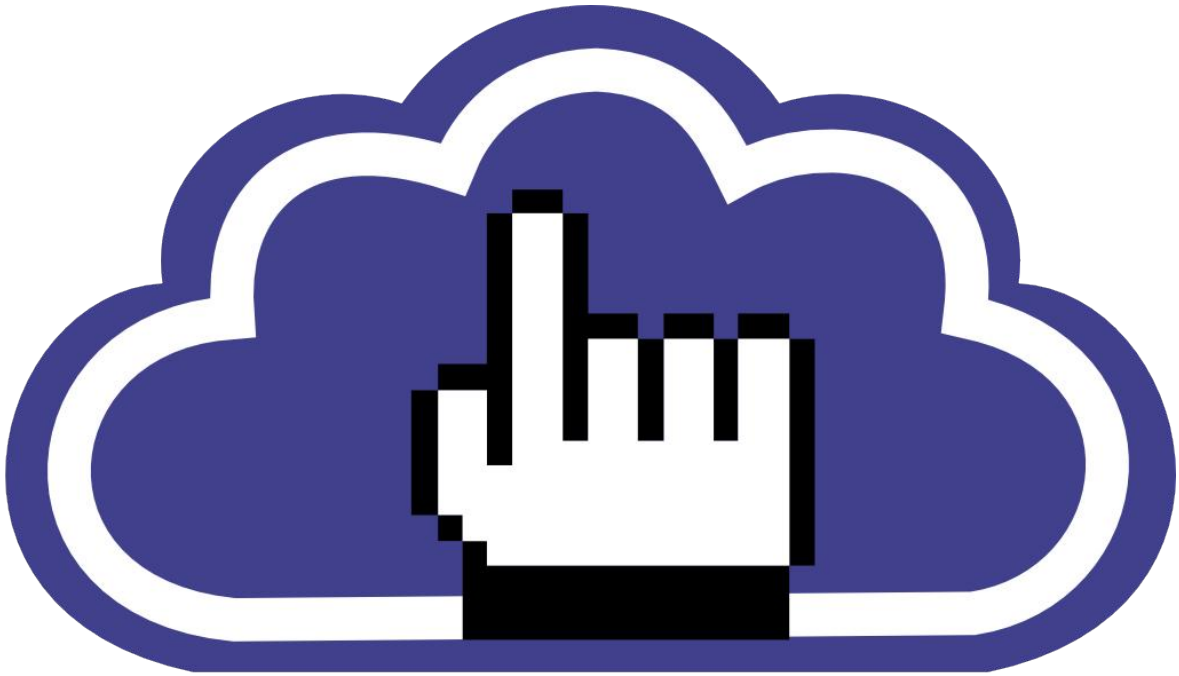


alcance libre

Configuración De Servidores Con GNU/Linux

Edición Octubre 2013

29 De Octubre De 2013

Joel Barrios Dueñas

Si este libro le ha sido de utilidad, puede contribuir al desarrollo de éste a través de suscripciones voluntarias a nuestro portal. Sus aportaciones nos ayudarán a crecer y desarrollar más y mejor contenido en el sitio de red y para mejorar este libro.

http://www.alcancelibre.org/staticpages/index.php/suscripciones

Alcance Libre ofrece **soporte técnico gratuito** exclusivamente a través de nuestros foros localizados en:

http://www.alcancelibre.org/forum/

Para cualquier consulta a través de otros medios, como correo electrónico, teléfono o mensajería instantánea, ofrecemos un **servicio comercial de consultoría**.

Alcance Libre ofrece los siguientes productos y servicios basados sobre Software Libre, gracias a los cuales financia sus operaciones. Para mayor información, estamos disponibles a través del número telefónico (52) (55) 5677-7130 de la ciudad de México o bien directamente en nuestras oficinas centrales en Serapio Rendón #63, oficina 4, Colonia San Rafael, Delegación Cuauhtemoc, C.P. 06470, México, D.F.

- Capacitación (cursos)
- Conferencias y pláticas
- Consultoría
- Implementaciones (Servidores)
- Soporte Técnico
- Publicidad en el portal

A mi difunto padre, a quien debo reconocer jamás supe comprender y a quien jamás le dí la oportunidad de entenderme.

Blanca, eres el amor de mi vida y gracias a ti inicié mi gusto por escribir. Te agradezco el haberme permitido escribirte todas esas cosas hace tantos años y el que hoy seas mi compañera en la vida.

A mis hijos, Joel Alejandro Barrios Caullieres y Sergio Armando Barrios Caullieres.

Ai

Conformación.

Me encuentro de regreso en mis raíces,
reviso mis trabajos pasados,
entre risas y otros cursis versos
(sueños entonces de adolescente),
desde existenciales a lo absurdo,
ligerezas tan sentimentales
construyendo un carácter (mi mundo).

Acerca de Joel Barrios Dueñas.

Hay poco que decir respecto de mí. Solía ser médico veterinario zootecnista, dedicado principalmente a la atención médica de pequeñas especies y otras mascotas (perros, gatos, peces y tortugas) y a la venta de alimentos y accesorios para mascotas. Trabajo activamente con computadoras personales desde 1990, con las cuales siempre he tenido gran facilidad. Mi primera computadora, fue una Apple IIe que me prestó un amigo y que eventualmente me vendió. Curiosamente, salvo por una clase que tomé en tercero de secundaria, durante la cual nos impartieron una introducción a la programación en BASIC y el uso general de computadoras Comodore 16, jamás he tomado un curso o capacitación relacionada con la informática o computación. Siempre he sido auto-didáctica.

Utilizo GNU/Linux desde Febrero de 1998 y desde Junio de 1999 como única plataforma en mi trabajo diario. Creo que es más que evidente que equivoque de carrera.

Gran parte de las razones de mi incursión en el mundo de la informática fueron verdaderamente incidentales. En 1997, nunca hubiera imaginado que me estaría ganado la vida en un ámbito completamente distinto al que me dedicaba durante ese tiempo. Yo ya tenía un consultorio veterinario y negocio pequeño de distribución de alimentos para mascotas, los cuales me aseguraban un ingreso regular y constante. Lamentablemente las condiciones del mercado durante el siguiente año repercutieron de forma importante en mis ingresos y fue entonces que empecé a buscar alternativas. Durante 1999 me estuve dedicando a la venta de equipo de cómputo y algo de diseño de sitios de red. Fueron algunos meses durante los cuales pude sobrevivir gracias a mis ahorros y a la suerte de contar un con talento poco común con las computadoras.

¿Cómo empecé este proyecto?

A mediados de 1999, mientras visitaba a un buen amigo mío, tuve un encuentro amistoso de unos 10 minutos con quien fue, en algún momento, la persona más importante que ha habido en mi vida, Blanca.

Yo subía por un elevador, divagando en mis pensamientos con sutilezas y otros menesteres relacionados con mi profesión de veterinario. Salí del ascensor y me dirigí hacia la puerta de mi amigo. Me detuve unos instantes antes de pulsar el botón del timbre. Había una extraña sensación que circundaba mi mente, como un aroma familiar que no era posible recordar. Mi amigo tenía una reunión con varias personas, algunas de las cuales yo conocía desde hacía algunos años pero que por diversas circunstancias no frecuentaba, así que supuse que era solo la sensación de volver a ver a personas después de mucho tiempo. Toque el timbre y un instante después mi amigo abrió la puerta. Le saludé con un apretón de manos y tras saludarle de la acostumbrada forma cortés, quedé mudo al ver que la chica de la que me había enamorado durante mis años de preparatoria, estaba presente. Frente a mi, sonriendo y mirándome.

Habían pasado varios años desde la última vez que nos habíamos visto. Conversamos un poco mientras ella cargaba al perro de mi amigo, al cual me disponía a aplicar una vacuna. Fue difícil dejar de mirarle y lo fue también el gusto de volver a verle de nuevo. Me despedí, pues tenía otro compromiso, pero en mi mente quedó un sentimiento de alegría de ver que aquella persona que había tenido un gran impacto en mi vida, estaba bien, muy hermosa y, en apariencia, feliz.

Fue ese breve encuentro el que me inspiró algunos meses después a crear algo que me proporcionara los medios para lograr hacer algo importante en vida. Fue ese deseo de ser alguien y tener algo que ofrecer si algún día y si las circunstancias lo permitían, buscar una segunda oportunidad con la persona de la que me había enamorado muchos años atrás y que de alguna forma jamás olvidé. Fue así que tras pasar muchas semanas planeando y tratando de dar forma a las ideas, el proyecto de comunidad que inicié con Linux Para Todos un 27 de agosto de 1999 y que hoy en día continuo con **Alcance Libre**. Surgió como un sueño, se materializó, se desarrollo y creció más allá de lo que hubiera imaginado.

Es irónico que años después, mi reencuentro con Blanca, quien es hoy en día mi esposa y madre de mis hijos Joel Alejandro y Sergio Armando, coincidiera con el fin del ciclo de Linux Para Todos, aunque también coincide con el inicio de otros proyectos y una nueva etapa con **Alcance Libre**.

Esta obra, que ahora comparto con los lectores, constituye la culminación del trabajo de más de 10 años de investigación y experiencias. Mucho del material que le compone fue escrito durante diferentes etapas de mi ciclo mientras fui propietario y administrador de Linux Para Todos. El fin de dicho ciclo me da la oportunidad de explorar otras áreas de la informática desde un diferente enfoque, mismo que se verá reflejado en el material actualizado que compone esta obra. Nunca me ha interesado ser famoso o un millonario.

Respecto del futuro, tengo una percepción distinta acerca de trascender más allá de los recuerdos familiares y trascender en la historia. Tal vez algún día, tal vez cien años después de haya muerto, se que de alguna forma mi legado en la historia será a través de todo lo que escribí y las cosas que pensaba y aquellas en las que creía.

Currículo.

Datos personales

- Nombre: Joel Barrios Dueñas.
- Año y lugar de nacimiento: 1970, México, Distrito Federal.
- Sexo: masculino.
- Estado civil: Unión Libre.

Escolaridad

- Secundaria: Colegio México (Acoxpa). 1982-1985
- Preparatoria: Instituto Centro Unión. 1985-1988
- Facultad de Medicina Veterinaria y Zootecnia, U.N.A.M. 1989-1993

Empleos en los que me he desempeñado.

- 1993-1999
    - Mi propia sub-distribuidora de alimentos y accesorios para mascotas. Dirección general.
    - Visitador Médico y asesor en informática. Distribuidora de Alimentos para Pequeñas Especies (Dialpe). Junio 1997 - Noviembre 1997.
    - Consultor externo de Dialpe 1998 – 1999.
- 1999 a 2006:
    - Fui el creador, director y administrador LinuxParaTodos.net.
    - Asesoría y consultoría en GNU/Linux.
    - Capacitación en GNU/Linux.
- 2002 - 2003:
    - Director Operativo Grupo MPR S.A. de C.V. (Actualmente Buytek Network Solutions)
- 2002 a 2006:
    - Director del proyecto LPT Desktop.
- 2007 a la fecha:
        - Director de proyecto AL Desktop (descartado).
        - Director de proyecto AL Server.
        - Director de proyecto ALDOS.
        - Fundador y director de proyecto de AlcanceLibre.org
        - Director del área de soporte técnico de Buytek Network Solutions.

Capacidades

- Inglés 99%
- Ensamble, configuración y mantenimiento de computadoras personales.
- Lenguajes HTML 4.0, HTML5 y CSS 2.0
- Programación en BASH
- Instalación, configuración y administración de Linux y servicios que trabajan sobre éste (Samba, Apache, Sendmail, Postfix, ClamAV, OpenLDAP, NFS, OpenSSH, VSFTPD, Shorewall, SNMP, MRTG, Squid, etc.)

Certificados

- Novell Certified Linux Desktop Administrator (Novell CLDA).
- Novell Certified Linux Administrator (Novell CLA).

Índice de contenido

1.¿Que es GNU/Linux?....34
1.1.Requerimientos del sistema....35

2.Estándar de Jerarquía de Sistema de Archivos....36
2.1.Introducción....36
2.2.Estructura de directorios....36
2.3.Particiones recomendadas para instalar CentOS, Fedora™, Red Hat™ Enterprise Linux, openSUSE™ y SUSE™ Linux Enterprise....38
2.4.Bibliografía....39

3.Procedimiento de instalación de CentOS 6....40
3.1.Procedimientos....40
3.1.1.Planeación....40
Obtención de los medios....40
3.1.2.Instalación del sistema operativo....40
3.2.Posterior a la instalación....74

4.Ajustes posteriores a la instalación de CentOS 6....75
4.1.Procedimientos....75
4.1.1.Nombres de los dispositivos de red....75
4.1.2.Dispositivos de red inactivos....76
4.1.3.Localización....77
4.1.4.Desactivar Plymouth....78
4.1.5.Instalar y habilitar, el modo gráfico....80
4.1.6.Ajustar la zona horaria, fecha y hora del sistema....82

5.Planificadores de Entrada/Salida en Linux....85
5.1.Introducción....85
5.2.Planificadores de Entrada/Salida disponibles en el núcleo de Linux....85
5.2.1.Anticipatory....85
5.2.2.CFQ....86
5.2.3.Deadline....87
5.2.4.Noop....88
5.3.¿Cuál planificador de Entrada/Salida elegir?....89
5.4.Bibliografía....90

6.Uso del disco de rescate de CentOS 6....91
6.1.Procedimientos....91

7.Iniciando el sistema en nivel de ejecución 1 (nivel mono-usuario)....102
7.1.Introducción....102
7.2.Procedimientos....102

8.Gestión de servicios....108
8.1.Introducción....108
8.2.Niveles de ejecución....108
8.3.Activar, desactivar, iniciar, detener o reiniciar servicios....114
8.3.1.En CentOS, Fedora™ y Red Hat™ Enterprise Linux....114
8.3.2.En openSUSE™ y SUSE™ Linux Enterprise....118

9.Gestión de espacio de memoria de intercambio (swap) en GNU/Linux....122
9.1.Introducción....122
9.1.1.Algo de historia....122
9.1.2.¿Qué es y como funciona el espacio de intercambio?....122
9.1.3.Circunstancias en lasque se requiere aumentar la cantidad de memoria de intercambio....122
Procedimientos....123
9.1.4.Cambiar el tamaño de la partición....123
9.1.5.Crear un archivo para memoria de intercambio....123
9.2.Procedimientos....123
9.2.1.Activar una partición de intercambio adicional....123
9.2.2.Utilizar un archivo como memoria de intercambio....124
9.2.3.Optimizando el sistema, cambiando el valor de /proc/sys/vm/swappiness....125

10.Procedimientos de emergencia....127
10.1.Introducción....127
10.2.Disco de rescate....127
10.3.Verificación de la integridad del disco....127
10.4.Respaldo y restauración del sector de arranque maestro....129
10.5.Asignación de formato de las particiones....130

11.Gestión de volúmenes lógicos....131
11.1.Introducción....131
Procedimientos....131
11.1.1.Crear un volumen lógico a partir de un disco duro nuevo....131
11.1.2.Añadir un volumen físico a un volumen lógico existente, a partir de espacio libre sin particionar en un disco duro....134
11.1.3.Quitar una unidad física a un volumen lógico....136
11.2.Bibliografía....139

12.Gestión de RAID a través de MDADM....140
12.1.Introducción....140
12.1.1.Tipos de arreglos soportados....140
Equipamiento lógico necesario....141
12.2.Procedimientos....142
12.2.1.Crear un arreglo tipo RAID1....142
12.2.2.Crear un arreglo tipo RAID10....148
12.2.3.Eliminar una unidad de almacenamiento de un arreglo....152
12.2.4.Eliminar un arreglo del sistema....154
12.3.Otras alternativas para gestionar MDADM....155

13.Optimización de sistemas de archivos ext3 y ext4....156
13.1.Introducción....156
13.1.1.Acerca de Ext3....156
13.1.2.Acerca de Ext4....156
13.1.3.Acerca del registro por diario (journaling)....156
13.2.Procedimientos....156
13.2.1.Utilizando el mandato e2fsck....157
13.2.2.Opciones de montado....157
13.2.3.Convirtiendo particiones de Ext3 a Ext4....161
13.2.4.Eliminando el registro por diario (journal) de Ext4....163
13.3.Bibliografía....164

14.Cifrado de particiones con LUKS....166
14.1.Introducción....166
14.2.Equipamiento lógico necesario....166
14.2.1.En CentOS, Fedora y Red Hat Enterprise Linux....166
14.2.2.En openSUSE y SUSE Linux Enterprise....166

14.3.Procedimientos....166
14.3.1.Cifrado de una partición existente en CentOS, Fedora™ y Red Hat™ Enterprise Linux....167
14.3.2.Cifrado de una partición existente en openSUSE™ y SUSE™ Linux Enterprise....169
14.3.3.Cifrado de una unidad de almacenamiento externo USB....176

15.Configuración y uso de sudo....179
15.1.Introducción....179
15.1.1.Historia....179
15.1.2.Acerca de sudo....179
15.2.Equipamiento lógico necesario....180
15.2.1.Instalación en CentOS, Fedora y Red Hat™ Enterprise Linux....180
15.2.2.Instalación en openSUSE y SUSE Linux Enterprise....180
15.3.Archivo /etc/sudoers....181
15.3.1.Cmnd_Alias....181
15.3.2.User_Alias....182
15.3.3.Host_Alias....182
15.3.4.Runas_Alias....182
15.4.Candados de seguridad....184
15.5.Lo más recomendado....185
15.5.1.Lo menos recomendado....185
15.6.Uso del mandato sudo....186
15.7.Facilitando la vida con aliases....188
15.7.1.CentOS, Fedora y Red Hat Enterprise Linux....188
15.7.2.En openSUSE y SUSE Linux Enterprise....189

16.Gestión de cuentas de usuario....190
16.1.Introducción....190
16.2.Procedimientos....190
16.2.1.Gestión de cuentas de usuario....190
16.2.2.Gestión de Grupos....191
16.2.3.Opciones avanzadas....191
16.3.Comentarios finales acerca de la seguridad....196
16.4.Configurando valores predeterminados para el alta de cuentas de usuario....198
16.4.1.Archivo /etc/default/useradd....198
16.4.2.Directorio /etc/skel....199
16.5.Ejercicio: Creando cuentas de usuario....201
16.5.1.Introducción....201
16.5.2.Procedimientos....201

17.Breve lección de mandatos básicos....203
17.1.Introducción....203
17.2.Procedimientos....203
17.2.1.Cambiar de usuario a super-usuario....203
17.2.2.Ver información del sistema y usuarios....204
17.2.3.Operaciones con archivos y directorios....205
17.2.4.Consultar ayuda, páginas de manual e información....216
17.2.5.Visualizando contenido de archivos....218
17.2.6.Enlaces físicos y simbólicos....222
17.2.7.Bucles....224
17.2.8.Aliases....227
17.2.9.Apagado y reinicio de sistema....228

18.Compresión y descompresión de archivos....230
18.1.Introducción....230
18.1.1.Acerca de ZIP....230
18.1.2.Acerca de TAR....230
18.1.3.Acerca de GZIP....230
18.1.4.Acerca de BZIP2....230

18.1.5.Acerca de XZ....230
18.2.Procedimientos....231
18.2.1.Preparativos....231
18.2.2.Compresión y descompresión de archivos *.zip....231
18.2.3.Creación y extracción de archivos *.tar....232
18.2.4.Compresión y descompresión de archivos *.tar.gz....232
18.2.5.Compresión y descompresión de archivos *.tar.bz2....233
18.2.6.Compresión y descompresión de archivos *.tar.xz....233
18.2.7.Crear respaldos del sistema de archivos....234

19.Gestión de procesos y trabajos....237
19.1.Introducción....237
19.2.Procedimientos....237
19.2.1.Uso de jobs, bg y fg....237
19.2.2.Uso de ps, kill y killall....239
19.2.3.Uso de nice y renice....242
19.2.4.Uso del mandato taskset....244
19.2.5.Uso del mandato top....246

20.Uso del mandato lsof....248
20.1.Introducción....248
20.1.1.Acerca de lsof....248
20.2.Equipamiento lógico necesario....248
20.2.1.En CentOS, Fedora™ y Red Hat™ Enterprise Linux....248
20.2.2.En openSUSE™ y SUSE™ Linux Enterprise....248
20.3.Procedimientos....248

21.Funciones básicas de vi....251
21.1.Introducción....251
21.2.Procedimientos....251
21.2.1.Equipamiento lógico necesario....251
21.3.Conociendo vi....251
21.4.Otros mandatos de vi....264
21.5.Más allá de las funciones básicas....265

22.Introducción a sed....266
22.1.Introducción....266
22.1.1.Acerca de sed....266
22.2.Procedimientos....266
22.3.Bibliografía....270

23.Introducción a AWK....271
23.1.Introducción....271
23.1.1.Acerca de AWK....271
23.1.2.Estructura de los programas escritos en AWK....271
23.2.Procedimientos....272

24.Uso de los mandatos chown y chgrp....277
24.1.Introducción....277
24.2.Mandato chown....277
24.2.1.Opciones....277
24.2.2.Utilización....277
24.3.Mandato chgrp....277
24.3.1.Opciones....278
24.3.2.Utilización....278
24.4.Ejemplos....278

25.Permisos del Sistema de Archivos en GNU/Linux....279
25.1.Introducción....279
25.2.Notación simbólica....279
25.3.Notación octal....280
25.3.1.Máscara de usuario....280
25.3.2.Permisos adicionales....282
25.4.Ejemplos....283
25.4.1.Ejemplos permisos regulares....283
25.4.2.Ejemplos permisos especiales....283
25.5.Uso del mandato chmod....283
25.5.1.Opciones del mandato chmod....284
25.5.2.El mandato chmod y los enlaces simbólicos....285

26.Listas de control de acceso y uso de los mandatos getfacl y setfacl....286
26.1.Introducción....286
26.2.Equipamiento lógico necesario....286
26.2.1.En CentOS, Fedora™ y Red Hat™ Enterprise Linux....286
26.2.2.En openSUSE™ y SUSE™ Enterprise Linux....287
26.3.Procedimientos....287

27.Uso del mandato chattr....292
27.1.Introducción....292
27.1.1.Acerca del mandato chattr....292
27.2.Opciones....292
27.3.Operadores....292
27.4.Atributos....293
27.5.Uso del mandato chattr....293
27.5.1.Ejemplos....293

28.Uso del mandato rpm....296
28.1.Introducción....296
28.1.1.Acerca de RPM....296
28.2.Procedimientos....296
28.2.1.Reconstrucción de la base de datos de RPM....296
28.2.2.Consulta de paquetes instalados en el sistema....296
28.2.3.Instalación de paquetes....299
28.2.4.Desinstalación de paquetes....305

29.Uso del mandato yum....306
29.1.Introducción....306
29.1.1.Acerca de YUM....306
29.2.Procedimientos....306
29.2.1.Listados....306
29.2.2.Búsquedas....307
29.2.3.Consulta de información....307
29.2.4.Instalación de paquetes....307
29.2.5.Desinstalación de paquetes....309
29.2.6.Actualizar sistema....310
29.2.7.Limpieza del directorio de cache....311
29.2.8.Verificación de la base de datos RPM....311

30.Configuración y uso de Crond....313
30.1.Introducción....313
30.1.1.Acerca del servicio crond....313
30.2.Equipamiento lógico necesario....314
30.2.1.En CentOS, Fedora™ y Red Hat™ Enterprise Linux....314
30.2.2.En openSUSE™....314

30.2.3.SUSE™ Linux Enterprise....315
30.2.4.Anacron....315
30.3.Procedimientos....315
30.3.1.Formato para el archivo /etc/crontab....316
Formato para utilizar con el mandato crontab -e....316
30.3.2.Ejemplos de configuraciones....317

31.Configuración y uso de Atd....319
31.1.Introducción....319
31.1.1.Acerca de los mandatos at y batch....319
31.2.Equipamiento lógico necesario....319
31.2.1.En CentOS, Fedora™ y Red Hat™ Enterprise Linux....319
31.2.2.En openSUSE™ y SUSE™ Linux Enterprise....319
31.3.Procedimientos....320
31.3.1.Archivos de configuración /etc/at.allow y /etc/at.deny....320
31.3.2.Directorio /var/spool/at....320
31.3.3.Mandato at....320
31.3.4.Mandato batch....321
31.3.5.Mandato atq....322
31.3.6.Mandato atrm....322

32.Asignación de cuotas en el sistema de archivos....323
32.1.Introducción....323
32.1.1.Acerca de las cuotas....323
32.1.2.Acerca de Inodos....323
32.1.3.Acerca de Bloques....323
32.2.Equipamiento lógico necesario....323
32.2.1.En CentOS, Fedora™ y Red Hat™ Enterprise Linux....323
32.2.2.En openSUSE™ y SUSE™ Enterprise Linux....324
32.3.Procedimientos....324
32.3.1.Edquota....325
32.4.Comprobaciones....327

33.Introducción a TCP/IP....329
33.1.Introducción....329
33.2.Niveles de pila....329
33.2.1.Modelo TCP/IP....329
33.2.2.Modelo OSI....335

34.Introducción a IP versión 4....336
34.1.Introducción....336
34.2.Direcciones....336
34.2.1.Representación de las direcciones....336
34.3.Asignación....337
34.3.1.Bloques reservados....337
34.4.Referencia de sub-redes de IP versión 4....338
34.5.Referencias....339

35.Configuración de red en GNU/Linux....341
35.1.Introducción....341
35.2.Procedimientos....341
35.2.1.Nombres de los dispositivos....341
35.2.2.NetworkManager....342
35.2.3.Asignación de parámetros de red....343
35.2.4.Rutas estáticos....345
35.2.5.Función de Reenvío de paquetes para IP versión 4....346
35.2.6.Herramientas para el intérprete de mandatos....347

35.2.7.Direcciones IP secundarias....348
35.2.8.La función Zeroconf....349
35.3.Ejercicios....351
35.3.1.Rutas estáticas....351
35.3.2.Ejercicio: Direcciones IP secundarias....353

36.Configuración de VLANs....357
36.1.Introducción....357
36.2.Equipamiento lógico necesario....357
36.2.1.En CentOS, Fedora™ y Red Hat™ Enterprise Linux....357
36.3.Procedimientos....357
36.3.1.Administrando direcciones IP de las VLANs a través de un servidor DHCP....361

37.Cómo configurar acoplamiento de tarjetas de red (bonding)....363
37.1.Introducción....363
37.2.Procedimientos....363
37.2.1.Archivo de configuración /etc/modprobe.conf....363
37.2.2.Archivo de configuración /etc/sysconfig/network-scripts/bond0....365
37.2.3.Iniciar, detener y reiniciar el servicio network....365
37.3.Comprobaciones....366
37.4.Bibliografía....367

38.Conexión a redes inalámbricas (Wifi) desde terminal....368
38.1.Introducción....368
38.1.1.¿Que es WPA? ¿Por qué debería usarlo en lugar de WEP?....368
38.2.Equipamiento lógico necesario....369
38.2.1.Instalación a través de yum....369
38.2.2.Preparativos....369
38.2.3.Autenticando en el punto de acceso....370
38.2.4.Asignando parámetros de red a la interfaz....371
38.3.Bibliografía....373

39.Uso del mandato nc (Netcat)....374
39.1.Introducción....374
39.1.1.Acerca de Netcat....374
39.2.Equipamiento lógico necesario....374
39.2.1.En CentOS, Fedora™ y Red Hat™ Enterprise Linux....374
39.2.2.En openSUSE™ y SUSE™ Linux Enterprise....374
39.3.Procedimientos en CentOS, Fedora™ y Red Hat™ Enterprise Linux....374
39.3.1.Conexiones simples....374
39.3.2.Revisión de puertos....375
39.3.3.Creando un modelo cliente servidor....376
39.3.4.Transferencia de datos....376
39.4.Procedimientos en openSUSE™ y SUSE™ Linux Enterprise....376
39.4.1.Conexiones simples....376
39.4.2.Revisión de puertos....377
39.4.3.Creando un modelo cliente servidor....378
39.4.4.Transferencia de datos....378

40.Como utilizar Netstat....379
40.1.Introducción....379
40.1.1.Acerca de Netstat....379
40.2.Procedimientos....379

41.Uso del mandato ARP....383
41.1.Introducción....383
41.1.1.Acerca de ARP....383

41.2.Equipamiento lógico necesario....384
41.3.Procedimientos....384

42.Introducción a IPTABLES....386
42.1.Introducción....386
42.1.1.Acerca de Iptables y Netfilter....386
42.2.Equipamiento lógico necesario....386
42.2.1.Instalación a través de yum....386
42.3.Procedimientos....386
42.3.1.Cadenas....386
42.3.2.Reglas de destino....386
42.3.3.Políticas por defecto....387
42.3.4.Limpieza de reglas específicas....387
42.3.5.Reglas específicas....387
Ejemplos de reglas....387
42.3.6.Eliminar reglas....389
42.3.7.Mostrar la lista de cadenas y reglas....389
42.3.8.Iniciar, detener y reiniciar el servicio iptables....390
42.3.9.Agregar el servicio iptables al arranque del sistema....391
42.4.Bibliografía....391

43.Configuración básica de Shorewall....392
43.1.Introducción....392
43.1.1.Acerca de Shorewall....392
43.1.2.Acerca de iptables y Netfilter....392
43.1.3.Acerca de iproute....392
43.2.Conceptos requeridos....392
43.2.1.¿Qué es una zona desmilitarizada?....392
43.2.2.¿Que es una Red Privada?....393
43.2.3.¿Qué es un NAT?....393
43.2.4.¿Qué es un DNAT?....393
43.3.Equipamiento lógico necesario....394
43.4.Procedimientos....394
43.4.1.Shorewall y SELinux....394
43.4.2.Activación de reenvío de paquetes para IPv4....395
43.4.3.Procedimiento de configuración de Shorewall....396
43.4.4.Iniciar, detener y reiniciar el servicio shorewall....401
43.4.5.Agregar el servicio shorewall al arranque del sistema....401

44.Cómo instalar y utilizar ClamAV en CentOS....402
44.1.Introducción....402
44.1.1.Acerca de ClamAV....402
44.2.Equipamiento lógico necesario....402
44.2.1.Creación del usuario para ClamAV....402
44.2.2.Instalación a través de yum....402
44.3.Procedimientos....403
44.3.1.SELinux y el servicio clamav-milter....403
44.3.2.Configuración de Freshclam....403
44.3.3.Uso básico del mandato clamscan....404

45.Instalación y configuración de CUPS....406
45.1.Introducción....406
45.1.1.Acerca de CUPS....406
45.2.Equipamiento lógico necesario....406
45.2.1.En CentOS, Fedora™ y Red Hat Enterprise™ Linux....406
45.2.2.En openSUSE™ y SUSE™ Linux Enterprise....407
45.3.Iniciar servicio y añadir el servicio al arranque del sistema....407
45.3.1.En CentOS, Fedora™ y Red Hat™ Enterprise Linux....408

45.3.2.En openSUSE™ y SUSE™ Linux Enterprise....408
45.4.Modificaciones necesarias en el muro cortafuegos....408
45.4.1.En CentOS, Fedora™ y Red Hat Enterprise™ Linux....408
45.4.2.En openSUSE™ y SUSE™ Linux Enterprise....410
45.5.Archivos y directorios de configuración....411
Archivos de bitácoras....412
Permitir conexiones desde anfitriones remotos....412
45.5.1.En CentOS, Fedora™ o Red Hat Enterprise™....412
45.5.2.En openSUSE™ o SUSE™ Linux Enterprise....413
45.5.3.Modo terminal....415
45.6.Añadir o modificar impresoras....416
45.6.1.Configuración de opciones de impresión....419
45.7.Impresión desde el intérprete de mandatos....420
45.8.Verificar estados de las colas de impresión....421
45.8.1.Cancelación de trabajos de impresión....422

46.Introducción al protocolo DNS....424
46.1.Equipamiento lógico necesario....424
46.2.Conceptos....424
46.2.1.Acerca del protocolo DNS (Domain Name System)....424
46.2.2.¿Qué es un NIC (Network Information Center)?....424
46.2.3.¿Qué es un FQDN (Fully Qualified Domain Name)?....424
46.2.4.Componentes de DNS....425
46.2.5.Herramientas de búsqueda y consulta....427
46.3.Modificaciones necesarias en el muro cortafuegos....428
46.3.1.System-config-firewall....428
46.3.2.Servicio iptables....429
46.3.3.Shorewall....429

47.Configuración de servidor de nombres de dominio (DNS)....431
47.1.Introducción....431
47.1.1.Acerca de Bind (Berkeley Internet Name Domain)....431
47.2.Equipamiento lógico necesario....431
47.2.1.Instalación a través de yum....431
47.2.2.Firma digital del servidor....432
47.2.3.Actualice el archivo de cache con los servidores DNS raíz....432
47.3.Procedimientos....433
47.3.1.SELinux y el servicio named....433
47.3.2.Configuración mínima para el archivo /etc/named.conf....434
47.3.3.Preparativos para añadir dominios....436
47.3.4.Creación de los archivos de zona....436
47.3.5.Seguridad adicional en DNS para uso público....440
47.3.6.Seguridad adicional en DNS para uso exclusivo en red local....446
47.3.7.Las zonas esclavas....447
47.3.8.Seguridad adicional para transferencias de zona....449
47.3.9.Reiniciar servicio y depuración de configuración....452

48.Configuración de servidor DHCP....454
48.1.Introducción....454
48.1.1.Acerca del protocolo DHCP....454
48.1.2.Acerca de dhcp por Internet Software Consortium, Inc....454
48.2.Equipamiento lógico necesario....455
48.2.1.CentOS, Fedora™ y Red Hat™ Enterprise Linux....455
48.3.Modificaciones necesarias en el muro cortafuegos....455
48.3.1.Servicio iptables....455
48.3.2.Shorewall....455
48.4.SELinux y el servicio dhcpd....456
48.5.Iniciar, detener y reiniciar, el servicio dhcpd....456

48.6.Procedimientos....457
48.6.1.Archivo de configuración /etc/sysconfig/dhcpd....457
48.6.2.Archivo de configuración dhcpd.conf....457
48.6.3.Configuración básica....457
48.6.4.Asignación de direcciones IP estáticas....458
48.6.5.Limitar el acceso por dirección MAC....459
48.6.6.Configuración para funcionar con DNS dinámico....460
48.7.Comprobaciones desde cliente DHCP....465

49.Instalación y configuración de vsftpd....467
49.1.Introducción....467
49.1.1.Acerca del protocolo FTP....467
49.1.2.Acerca del protocolo FTPS....467
49.1.3.Acerca de RSA....468
49.1.4.Acerca de OpenSSL....468
49.1.5.Acerca de X.509....468
49.1.6.Acerca de vsftpd....468
49.2.Equipamiento lógico necesario....468
49.2.1.Instalación a través de yum....469
49.3.Archivos de configuración....469
49.3.1.Iniciar, detener y reiniciar el servicio vsftpd....469
49.3.2.Agregar el servicio vsftpd al arranque del sistema....469
49.4.Modificaciones necesarias en el muro cortafuegos....470
49.4.1.Servicio iptables....470
49.4.2.Shorewall....470
49.5.Procedimientos....470
49.5.1.SELinux y el servicio vsftpd....470
49.5.2.Archivo /etc/vsftpd/vsftpd.conf....471
49.5.3.Opción anonymous_enable....471
49.5.4.Opción local_enable....472
49.5.5.Opción write_enable....472
49.5.6.Opciones anon_upload_enable y anon_mkdir_write_enable....472
49.5.7.Opción ftpd_banner....472
49.5.8.Estableciendo jaulas para los usuarios: opciones chroot_local_user y chroot_list_file....473
49.5.9.Opciones pasv_min_port y pasv_max_port....473
49.5.10.Control del ancho de banda....474

50.Configuración de OpenSSH....478
50.1.Introducción....478
50.1.1.Acerca de SSH....478
50.1.2.Acerca de SFTP....478
50.1.3.Acerca de SCP....478
50.1.4.Acerca de OpenSSH....478
50.2.Equipamiento lógico necesario....478
50.2.1.En CentOS, Fedora™ y Red Hat™ Enterprise Linux....479
50.2.2.En openSUSE™ y SUSE™ Linux Enterprise....479
50.3.Activar, desactivar, iniciar, detener y reiniciar el servicio ssh....479
50.3.1.En CentOS, Fedora™ y Red Hat™ Enterprise Linux....479
50.3.2.En openSUSE™ y SUSE™ Linux Enterprise....479
50.4.Modificaciones necesarias en el muro cortafuegos....480
50.4.1.En CentOS, Fedora™ y Red Hat™ Enterprise Linux....480
50.4.2.En openSUSE™ y SUSE™ Linux Enterprise....481
50.5.SELinux y el servicio sshd....481
50.5.1.Política ssh_chroot_rw_homedirs....482
50.5.2.Política fenced_can_ssh....482
50.5.3.Política ssh_chroot_manage_apache_content....482
50.5.4.Política ssh_sysadm_login....482
50.5.5.Política allow_ssh_keysign....482
50.5.6.Contexto ssh_home_t....482
50.6.Archivos de configuración....483

50.7.Procedimientos....483
50.7.1.Parámetro Port....484
50.7.2.Parámetro ListenAddress....484
50.7.3.Parámetro PermitRootLogin....484
50.7.4.Parámetro X11Forwarding....484
50.7.5.Parámetro AllowUsers....484
50.7.6.Parámetro UseDNS....485
50.8.Probando OpenSSH....485
50.8.1.Acceso con intérprete de mandatos....485
50.8.2.Transferencia de archivos a través de SFTP....485
50.8.3.Transferencia de archivos a través de SCP....487

51.OpenSSH con autenticación a través de firma digital....489
51.1.Introducción....489
51.2.Procedimientos....489
51.2.1.Modificaciones en el Servidor remoto....489
51.2.2.Modificaciones en el cliente....490
51.2.3.Comprobaciones....491

52.Configuración y uso de NTP....492
52.1.Introducción....492
52.1.1.Acerca de NTP....492
52.1.2.Acerca de UTC....493
52.2.Equipamiento lógico necesario....493
52.2.1.En CentOS, Fedora™ y Red Hat™ Enterprise Linux....493
52.2.2.En openSUSE™ y SUSE™ Linux Enterprise....493
52.3.Modificaciones necesarias en el muro cortafuegos....493
52.3.1.En CentOS, Fedora™ y Red Hat™ Enterprise Linux....493
52.3.2.En openSUSE™ y SUSE™ Linux Enterprise....495
52.4.Iniciar, detener y reiniciar el servicio ntpd....496
52.4.1.En CentOS, Fedora™ y Red Hat™ Enterprise Linux....496
52.4.2.En openSUSE™ y SUSE™ Linux Enterprise....496
52.5.Procedimientos....497
52.5.1.Herramienta ntpdate....497
52.5.2.Archivo de configuración /etc/ntp.conf....497
52.5.3.Configuración de clientes....501

53.Configuración de servidor NFS....505
53.1.Introducción....505
53.2.Equipamiento lógico necesario....505
53.2.1.En CentOS, Fedora y Red Hat Enterprise Linux....505
53.2.2.Instalación en openSUSE y SUSE Linux Enterprise....506
53.3.Definir los puertos utilizados por NFS....506
53.4.Iniciar servicio y añadir el servicio al inicio del sistema....507
53.4.1.En CentOS, Fedora y Red Hat Enterprise Linux....507
53.4.2.En openSUSE y SUSE Linux Enterprise....508
53.5.Modificaciones necesarias en los archivos /etc/hosts.allow y /etc/hosts.deny....508
53.6.Modificaciones necesarias en el muro cortafuegos....509
53.6.1.En CentOS, Fedora y Red Hat Enterprise Linux....510
53.6.2.En openSUSE y SUSE Linux Enterprise....512
53.7.Procedimientos....513
53.7.1.El archivo /etc/exports....513
53.7.2.Verificación del servicio....515
53.7.3.Montaje de sistemas de archivos NFS....517
53.7.4.Modulo nfs de YaST en openSUSE y SUSE Linux Enterprise....518
53.8.Ejercicios....518
53.8.1.Compartir un volumen NFS para acceso público....518
53.9.Bibliografía....520

54.Configuración básica de Samba....521
54.1.Introducción....521
54.1.1.Acerca del protocolo SMB....521
54.1.2.Acerca de Samba....521
54.2.Equipamiento lógico necesario....521
Instalación a través de yum....521
54.3.Modificaciones necesarias en el muro cortafuegos....522
54.3.1.Servicio iptables....522
54.3.2.Shorewall....522
54.4.SELinux y el servicio smb....523
54.5.Iniciar el servicio y añadirlo al arranque del sistema....524
54.6.Procedimientos....524
54.6.1.Alta de cuentas de usuario....524
54.6.2.El archivo lmhosts....525
54.6.3.Opciones principales del archivo smb.conf....526
54.6.4.Opción remote announce....527
54.6.5.Impresoras en Samba....528
54.6.6.Compartiendo directorios a través de Samba....528
54.7.Comprobaciones....530
54.7.1.Modo texto desde GNU/Linux....530
54.7.2.Modo gráfico....532

55.Cómo configurar Samba denegando acceso a ciertos archivos....534
55.1.Introducción....534
55.2.Procedimientos....534
55.3.Aplicando los cambios....534
55.4.Comprobaciones....535

56.Cómo configurar Samba con Papelera de Reciclaje....536
56.1.Introducción....536
56.2.Procedimientos....536
56.3.Aplicando los cambios....538
56.4.Comprobaciones....538

57.Cómo configurar Samba como cliente o servidor WINS....540
57.1.Introducción....540
57.2.Procedimientos....540
57.2.1.Parámetros wins server y wins support....540
57.2.2.Parámetro name resolve order....541
57.2.3.Parámetro wins proxy....541
57.2.4.Parámetro dns proxy....541
57.2.5.Parámetro max ttl....541
57.2.6.Parámetros max wins ttl y min wins ttl....541
57.3.Aplicando los cambios....542

58.Instalación, configuración y optimización de Spamassassin....543
58.1.Introducción....543
58.1.1.Acerca de SpamAssassin....543
58.1.2.Acerca de Procmail....543
58.2.Equipamiento lógico necesario....543
58.2.1.Instalación a través de yum....543
58.3.SELinux y el servicio spamasssassin....544
58.3.1.Políticas de SElinux....544
58.3.2.Otros ajustes de SELinux....544
58.4.Procedimientos....546
58.4.1.Iniciar el servicio y añadirlo a los servicios de arranque del sistema....546
58.4.2.Configuración de Procmail....546

58.4.3.Configuración del archivo /etc/mail/spamassassin/local.cf. 547
58.5.Consejos para sacarle mejor provecho a Spamassassin utilizando sa-learn. 549
58.6.Incrementando las capacidades de filtrado. 550
58.6.1.Optimizando Spamassassin. 551
58.6.2.¿Por qué Perl-Mail-SPF, Perl-Razor-Agent, Pyzor, Spamassassin-FuzzyOcr y poppler-utils? 551

59.Configuración simple para Antivirus y Antispam. 553
59.1.Procedimientos. 553

60.Introducción a los protocolos de correo electrónico. 558
60.1.Introducción. 558
60.1.1.Preparativos. 558
60.1.2.Protocolos utilizados. 560
60.2.Referencias. 563

61.Configuración básica de Sendmail. 565
61.1.Introducción. 565
61.1.1.Acerca de Sendmail. 565
61.1.2.Acerca de Dovecot. 565
61.1.3.Acerca de SASL y Cyrus SASL. 565
61.2.Equipamiento lógico necesario. 565
Instalación a través de yum. 566
61.3.Procedimientos. 566
61.3.1.Definiendo Sendmail como agente de transporte de correo predeterminado. 566
61.3.2.Alta de cuentas de usuario y asignación de contraseñas. 567
61.3.3.Dominios a administrar. 568
61.3.4.Control de acceso. 568
61.3.5.Alias de la cuenta del usuario root. 570
61.3.6.Configuración de funciones de Sendmail. 571
61.3.7.Configuración de Dovecot. 575
61.3.8.Añadir al inicio del sistema e iniciar servicios dovecot y sendmail. 576
61.4.Modificaciones necesarias en el muro cortafuegos. 577
61.4.1.Servicio iptables. 577
61.4.2.Shorewall. 578
61.5.Lecturas posteriores. 578

62.Configuración de Sendmail y Dovecot con soporte SSL/TLS. 579
62.1.Introducción. 579
62.1.1.Acerca de DSA. 579
62.1.2.Acerca de RSA. 579
62.1.3.Acerca de X.509. 579
62.1.4.Acerca de OpenSSL. 579
62.2.Procedimientos. 580
62.2.1.Generando firma digital y certificado para ambos servicios. 580
62.2.2.Configuración de Sendmail. 581
62.2.3.Configuración de Dovecot. 583
62.2.4.Comprobaciones. 584
62.2.5.Configuración de GNOME Evolution. 584
62.2.6.Configuración Mozilla Thunderbird. 586

63.Configuración avanzada de Sendmail. 588
63.1.Antes de continuar. 588
63.2.Usuarios Virtuales. 588
63.3.Encaminamiento de dominios. 589
63.3.1.Redundancia del servidor de correo. 590
63.3.2.Servidor de correo intermediario. 590
63.4.Verificando el servicio. 591

63.5.Pruebas de envío de correo....592
63.5.1.Utilizando nc....592
63.5.2.Utilizando mutt....594

64.Opciones avanzadas de seguridad para Sendmail....596
64.1.Introducción....596
64.2.Funciones....596
64.2.1.confMAX_RCPTS_PER_MESSAGE....596
64.2.2.confBAD_RCPT_THROTTLE....596
64.2.3.confPRIVACY_FLAGS....596
64.2.4.confMAX_HEADERS_LENGTH....597
64.2.5.confMAX_MESSAGE_SIZE....597
64.2.6.confMAX_DAEMON_CHILDREN....597
64.2.7.confCONNECTION_RATE_THROTTLE....597

65.Instalación y configuración de Postfix y Dovecot con soporte para TLS y autenticación. 599
65.1.Introducción....599
65.1.1.Acerca de Postfix....599
65.1.2.Acerca de Dovecot....599
65.1.3.Acerca de SASL y Cyrus SASL....599
65.1.4.Acerca de DSA....600
65.1.5.Acerca de RSA....600
65.1.6.Acerca de X.509....600
65.1.7.Acerca de OpenSSL....600
65.2.Equipamiento lógico necesario....600
65.3.Procedimientos....601
65.3.1.Definiendo Postfix como agente de transporte de correo predeterminado....601
65.3.2.SELinux y Postfix....601
65.3.3.Configuración de Postfix....602
65.3.4.Generando firma digital y certificado para ambos servicios....602
65.3.5.Configuración de Dovecot en CentOS 5 y Red Hat Enterprise Linux 5....605
65.3.6.Configuración de Dovecot en CentOS 6 y Red Hat Enterprise Linux 6....606
65.3.7.Iniciar servicios y añadir éstos al arranque del sistema....606
65.3.8.Soporte para LMTP....607
65.3.9.Modificaciones necesarias en el muro cortafuegos....607
65.3.10.Requisitos en la zona de reenvío en el servidor DNS....607
65.4.Comprobaciones....608
65.4.1.A través de terminal....608
65.4.2.A través de clientes de correo electrónico....608
65.5.Modificaciones necesarias en el muro cortafuegos....611

66.Cómo instalar y configurar Amavisd-new con Postfix en CentOS....613
66.1.Introducción....613
66.1.1.Acerca de Amavisd-new....613
66.2.Equipamiento lógico necesario....613
66.2.1.Creación del usuario para ClamAV....613
66.2.2.Configuración de depósitos YUM para CentOS 5 y Red Hat Enterprise Linux 5....613
66.3.Procedimientos....614
66.3.1.Configuración de SELinux....614
66.3.2.Configuración de Amavisd-new....615
66.3.3.Configuración de Postfix....615
66.3.4.Iniciar, detener y reiniciar el servicio spamass-milter....616
66.3.5.Postfix con dominios virtuales y Amavisd-new....617

67.Cómo configurar Postfix en CentOS para utilizar dominios virtuales con usuarios del sistema....618
67.1.Introducción....618

67.2.Procedimientos....618
67.2.1.Ajustes en el servicio saslauthd....618
67.2.2.Configuración de SELinux....619
67.2.3.Configuración de Postfix....621
67.2.4.Reiniciar el servicio postfix....623

68.Envío de correo a todos los usuarios del sistema....624
68.1.Procedimientos....624
68.2.Acerca de la seguridad....624

69.Cómo configurar clamav-milter....625
69.1.Introducción....625
69.1.1.Acerca de clamav-milter....625
69.1.2.Acerca de ClamAV....625
69.2.Equipamiento lógico necesario....625
69.2.1.Creación del usuario para ClamAV....626
69.2.2.Instalación a través de yum....626
69.3.Procedimientos....626
69.3.1.SELinux y el servicio clamav-milter....626
69.3.2.Requisitos previos....628
69.3.3.Archivo /etc/mail/sendmail.mc....628
69.3.4.Configuración....628
69.3.5.Iniciar, detener y reiniciar el servicio clamav-milter....628

70.Cómo configurar spamass-milter....630
70.1.Introducción....630
70.1.1.Requisitos previos....630
70.1.2.Acerca de spamass-milter....630
70.1.3.Acerca de SpamAssassin....630
70.2.Equipamiento lógico necesario....630
70.2.1.Instalación a través de yum....631
70.3.Procedimientos....631
70.3.1.SELinux y el servicio spamass-milter....631
70.3.2.Archivo /etc/mail/sendmail.mc....633
70.3.3.Archivo /etc/sysconfig/spamass-milter....634
70.3.4.Archivo /etc/procmailrc....635
Archivo /etc/sysconfig/spamassassin....635
70.3.5.Iniciar, detener y reiniciar el servicio spamass-milter....636

71.Introducción a OpenLDAP....637
71.1.Introducción....637
71.1.1.Acerca de LDAP....637
71.1.2.Acerca de RSA....637
71.1.3.Acerca de X.509....637
71.1.4.Acerca de OpenSSL....637

72.Configuración de OpenLDAP como servidor de autenticación....639
72.1.Introducción....639
72.2.Equipamiento lógico necesario....639
Instalación a través de yum....639
72.3.Procedimientos....639
72.3.1.SELinux y el servicio ldap....639
72.3.2.Certificados para TLS/SSL....640
72.3.3.Creación de directorios....641
72.3.4.Creación de claves de acceso para LDAP....641
72.3.5.Archivo de configuración /etc/openldap/slapd.conf....642
72.3.6.Inicio del servicio....644
72.3.7.Migración de cuentas existentes en el sistema....644

72.4.Comprobaciones....646
72.5.Configuración de clientes....647
72.6.Administración....648
72.7.Respaldo de datos....648
72.8.Restauración de datos....649
72.9.Modificaciones necesarias en el muro cortafuegos....650
72.9.1.Servicio iptables....650
72.9.2.Shorewall....651

73.Configuración básica de MySQL™....652
73.1.Introducción....652
73.1.1.Acerca de MySQL™....652
73.2.Equipamiento lógico necesario....652
73.2.1.En CentOS, Fedora™ y Red Hat™ Enterprise Linux....652
73.2.2.En openSUSE™ y SUSE™ Linux Enterprise....652
73.3.Modificaciones necesarias en el muro cortafuegos....652
73.3.1.En openSUSE™ y SUSE™ Linux Enterprise....654
73.4.SELinux y MySQL™, sólo en CentOS, Fedora™ y Red Hat™ Enterprise Linux....655
73.5.Procedimientos....655
73.5.1.Iniciar, detener y reiniciar el servicio mysqld....655
73.5.2.Archivos y directorios de configuración....656
73.5.3.Asignación de contraseña al usuario root en MySQL....656
73.5.4.Crear y eliminar bases de datos....658
73.5.5.Respaldo y restauración de bases de datos....658
73.5.6.Permisos de acceso a las bases de datos....658
73.6.Optimización de MySQL....660
73.6.1.Deshabilitar la resolución de nombres de anfitrión....660
73.6.2.Aumentar el tamaño de cache de consultas....661
73.6.3.Soporte para UTF-8....662
73.7.Bibliografía....663

74.Configuración básica de Apache....664
74.1.Introducción....664
74.1.1.Acerca del protocolo HTTP....664
74.1.2.Acerca de Apache....664
74.2.Equipamiento lógico necesario....664
74.2.1.En CentOS, Fedora™ y Red Hat™ Enterprise Linux....664
74.3.Iniciar servicio y añadir el servicio al arranque del sistema....665
74.4.SELinux y Apache....665
74.5.Modificaciones necesarias en el muro cortafuegos....667
74.5.1.Servicio iptables....667
74.5.2.Shorewall....668
74.6.Procedimientos....668
74.6.1.Archivos de configuración....668
74.6.2.UTF-8 y codificación de documentos....668
74.6.3.Directorios virtuales....669
74.6.4.Limitar el acceso a directorios por dirección IP....671
74.6.5.Limitar el acceso por usuario y contraseña....671
74.6.6.Asignación de directivas para PHP....673
74.6.7.Re-dirección de directorios....674
74.6.8.Tipos de MIME....675
74.6.9.Impedir enlace remoto de imágenes....675

75.Configuración de Apache con soporte SSL/TLS....678
75.1.Introducción....678
75.1.1.Acerca de HTTPS....678
75.1.2.Acerca de RSA....678
75.1.3.Acerca de Triple DES....678

75.1.4.Acerca de X.509....678
75.1.5.Acerca de OpenSSL....679
75.1.6.Acerca de mod_ssl....679
75.2.Requisitos....679
75.3.Equipamiento lógico necesario....679
75.3.1.Instalación a través de yum....679
75.4.Procedimientos....679
75.4.1.Generando firma digital y certificado....679
75.4.2.Configuración simple de Apache para un solo dominio....681
75.4.3.Configuración de Apache para múltiples dominios....682
75.4.4.Comprobación....683
75.4.5.Modificaciones necesarias en el muro cortafuegos....683

76.Configuración de Squid: Opciones básicas....685
76.1.Introducción....685
76.1.1.¿Qué es Servidor Intermediario (Proxy)?....685
76.1.2.Acerca de Squid....686
76.2.Equipamiento lógico necesario....686
76.2.1.Instalación a través de yum....686
76.3.SELinux y el servicio squid....686
76.4.Antes de continuar....687
76.5.Configuración básica....687
76.5.1.Controles de acceso....688
76.5.2.Aplicando Listas y Reglas de control de acceso....690
76.5.3.Opción cache_mgr....691
76.5.4.Opción http_port....692
76.5.5.Opción cache_dir....692
76.5.6.Opción maximum_object_size....693
76.5.7.Opciones cache_swap_low y cache_swap_high....693
76.5.8.Opción cache_replacement_policy....693
76.5.9.Opción cache_mem....694
76.6.Estableciendo el idioma de los mensajes mostrados por Squid hacia el usuario....694
76.7.Iniciando, reiniciando y añadiendo el servicio al arranque del sistema....695
76.8.Depuración de errores....695
76.9.Modificaciones necesarias en el muro cortafuegos....695
76.9.1.Re-direccionamiento de peticiones a través de la opción REDIRECT en Shorewall....696
76.9.2.Re-direccionamiento de peticiones a través de iptables....696

77.Configuración de Squid: Acceso por autenticación....697
77.1.Introducción....697
77.2.Equipamiento lógico necesario....697
Eligiendo el módulo de autenticación....697
77.2.1.Autenticación a través del módulo LDAP....697
77.2.2.Autenticación a través del módulo NCSA....698
77.3.Listas y reglas de control de acceso....699
77.3.1.Finalizando procedimiento....699

78.Configuración de Squid: Restricción de acceso a Sitios de Internet....701
78.1.Introducción....701
78.2.Restricción por expresiones regulares....701
78.3.Restricción por expresiones regulares....702
78.3.1.Permitiendo acceso a sitios inocentes incidentalmente bloqueados....703
78.3.2.Finalizando procedimiento....704

79.Configuración de Squid: Restricción de acceso a contenido por extensión....705
79.1.Introducción....705
79.2.Definiendo elementos de la Lista de Control de Acceso....705
79.2.1.Finalizando procedimiento....706

80.Configuración de Squid: Restricción de acceso por horarios....708
80.1.Introducción....708
80.2.Procedimientos....708
80.2.1.Más ejemplos....709
80.2.2.Finalizando procedimiento....710

81.Cómo configurar squid con soporte para direcciones MAC....711
81.1.Introducción....711
81.1.1.Acerca de Squid....711
81.2.Equipamiento lógico necesario....711
81.2.1.Instalación a través de yum....711
81.3.Procedimientos....711
Archivo /etc/squid/listas/macsredlocal....712
81.3.1.Archivo /etc/squid/squid.conf....712
81.4.Iniciar, detener y reiniciar el servicio squid....713

82.Configuración de Squid: Cachés en jerarquía....714
82.1.Introducción....714
82.1.1.Procedimientos....714

83.Configuración de WPAD....716
83.1.Introducción....716
83.1.1.Acerca de WPAD....716
83.2.Procedimientos....716
83.2.1.Equipamiento lógico necesario....716
83.2.2.Ajustes en el muro cortafuegos....717
83.2.3.Resolución local del nombre de anfitrión....718
83.2.4.Archivo wpad.dat....718
83.2.5.Configuración de Apache....719
83.2.6.Anuncio del archivo wpad.dat....720
83.2.7.Comprobaciones....722

84.Instalación y configuración de la herramienta de reportes Sarg....726
84.1.Introducción....726
84.2.Equipamiento lógico necesario....726
84.3.Procedimientos....726

85.Configuración de OpenVPN....730
85.1.Introducción....730
85.1.1.Acerca de OpenVPN....730
85.1.2.Breve explicación de lo que se logrará con este documento....730
85.2.Instalación del equipamiento lógico necesario....731
85.2.1.Instalación en CentOS....731
85.3.Procedimientos....731
85.3.1.Configuración de muro cortafuegos con Shorewall....735
85.3.2.Configuración de clientes Windows....737
85.3.3.Clientes GNU/Linux....739
85.4.Bibiliografía....745

86.Usando Smartd para anticipar los desastres de disco duro....746
86.1.Introducción....746
86.2.Procedimientos....746

87.Restricción de acceso a unidades de almacenamiento externo....748
87.1.Introducción....748

87.2.Procedimientos.....748
87.2.1.Bloquear el uso de unidades de disco óptico.....748
87.2.2.Bloquear uso del módulo usb-storage o uas del núcleo de Linux.....749
87.2.3.En CentOS, Fedora y Red Hat Enterprise Linux.....749
87.2.4.En openSUSE.....750
87.2.5.En SUSE Linux Enterprise.....750
87.2.6.Reglas de UDEV para impedir el acceso a unidades de almacenamiento USB.....751
87.2.7.PolicyKit para restringir el acceso a unidades de almacenamiento externo en general.....752

88.Administración de configuraciones de GNOME 2.....757
88.1.Introducción.....757
88.2.Mandato gconftool-2.....757
88.2.1.Configuraciones más comúnmente restringidas en el escritorio de GNOME.....760
Herramienta gconf-editor.....761

Notas.....762

Información de Derechos reservados de esta publicación.

Reconocimiento-NoComercial-CompartirIgual 2.1

Usted es libre de:

- copiar, distribuir y comunicar públicamente la obra
- hacer obras derivadas

Bajo las condiciones siguientes:

Reconocimiento. Debe reconocer y citar al autor original.

No comercial. No puede utilizar esta obra para fines comerciales.

Compartir bajo la misma licencia. Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta.

- Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra.
- Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor

Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior.

Reconocimiento-NoComercial-CompartirIgual 2.1

CREATIVE COMMONS CORPORATION NO ES UN DESPACHO DE ABOGADOS Y NO PROPORCIONA SERVICIOS JURÍDICOS. LA DISTRIBUCIÓN DE ESTA LICENCIA NO CREA UNA RELACIÓN ABOGADO-CLIENTE. CREATIVE COMMONS PROPORCIONA ESTA INFORMACIÓN TAL CUAL (ON AN "AS-IS" BASIS). CREATIVE COMMONS NO OFRECE GARANTÍA ALGUNA RESPECTO DE LA INFORMACIÓN PROPORCIONADA, NI ASUME RESPONSABILIDAD ALGUNA POR DAÑOS PRODUCIDOS A CONSECUENCIA DE SU USO.

Licencia

LA OBRA (SEGÚN SE DEFINE MÁS ADELANTE) SE PROPORCIONA BAJO TÉRMINOS DE ESTA LICENCIA PÚBLICA DE CREATIVE COMMONS ("CCPL" O "LICENCIA"). LA OBRA SE ENCUENTRA PROTEGIDA POR LA LEY ESPAÑOLA DE PROPIEDAD INTELECTUAL Y/O CUALESQUIERA OTRAS NORMAS RESULTEN DE APLICACIÓN. QUEDA PROHIBIDO CUALQUIER USO DE LA OBRA DIFERENTE A LO AUTORIZADO BAJO ESTA LICENCIA O LO DISPUESTO EN LAS LEYES DE PROPIEDAD INTELECTUAL.

MEDIANTE EL EJERCICIO DE CUALQUIER DERECHO SOBRE LA OBRA, USTED ACEPTA Y CONSIENTE LAS LIMITACIONES Y OBLIGACIONES DE ESTA LICENCIA. EL LICENCIADOR LE CEDE LOS DERECHOS CONTENIDOS EN ESTA LICENCIA, SIEMPRE QUE USTED ACEPTE LOS PRESENTES TÉRMINOS Y CONDICIONES.

1. Definiciones

a. La **"obra"** es la creación literaria, artística o científica ofrecida bajo los términos de esta licencia.

b. El **"autor"** es la persona o la entidad que creó la obra.

c. Se considerará **"obra conjunta"** aquella susceptible de ser incluida en alguna de las siguientes categorías:

   i. **"Obra en colaboración"**, entendiendo por tal aquella que sea resultado unitario de la colaboración de varios autores.

d. **"Obra colectiva"**, entendiendo por tal la creada por la iniciativa y bajo la coordinación de una persona natural o jurídica que la modifique y divulgue bajo su nombre y que esté constituida por la reunión de aportaciones de diferentes autores cuya contribución personal se funde en una creación única y autónoma, para la cual haya sido concebida sin que sea posible atribuir separadamente a cualquiera de ellos un derecho sobre el conjunto de la obra realizada.

e. **"Obra compuesta e independiente"**, entendiendo por tal la obra nueva que incorpore una obra preexistente sin la colaboración del autor de esta última.

f. Se considerarán **"obras derivadas"** aquellas que se encuentren basadas en una obra o en una obra y otras preexistentes, tales como: las traducciones y adaptaciones; las revisiones, actualizaciones y anotaciones; los compendios, resúmenes y extractos; los arreglos musicales y, en general, cualesquiera transformaciones de una obra literaria, artística o científica, salvo que la obra resultante tenga el carácter de obra conjunta en cuyo caso no será considerada como una obra derivada a los efectos de esta licencia. Para evitar la duda, si la obra consiste en una composición musical o grabación de sonidos, la sincronización temporal de la obra con una imagen en movimiento ("synching") será considerada como una obra derivada a los efectos de esta licencia.

g. Tendrán la consideración de **"obras audiovisuales"** las creaciones expresadas mediante una serie de imágenes asociadas, con o sin sonorización incorporada, así como las composiciones musicales, que estén destinadas esencialmente a ser mostradas a través de aparatos de proyección o por cualquier otro medio de comunicación pública de la imagen y del sonido, con independencia de la naturaleza de los soportes materiales de dichas obras.

h. El **"licenciador"** es la persona o la entidad que ofrece la obra bajo los términos de esta licencia y le cede los derechos de explotación de la misma conforme a lo dispuesto en ella.

i. **"Usted"** es la persona o la entidad que ejercita los derechos cedidos mediante esta licencia y que no ha violado previamente los términos de la misma con respecto a la obra o que ha recibido el permiso expreso del licenciador de ejercitar los derechos cedidos mediante esta licencia a pesar de una violación anterior.

j. La **"transformación"** de una obra comprende su traducción, adaptación y cualquier otra modificación en su forma de la que se derive una obra diferente. Cuando se trate de una base de datos según se define más adelante, se considerará también transformación la reordenación de la misma. La creación resultante de la transformación de una obra tendrá la consideración de obra derivada.

k. Se entiende por **"reproducción"** la fijación de la obra en un medio que permita su comunicación y la obtención de copias de toda o parte de ella.

l. Se entiende por **"distribución"** la puesta a disposición del público del original o copias de la obra mediante su venta, alquiler, préstamo o de cualquier otra forma.

m. Se entenderá por **"comunicación pública"** todo acto por el cual una pluralidad de personas pueda tener acceso a la obra sin previa distribución de ejemplares a cada una de ellas. No se considerará pública la comunicación cuando se celebre dentro de un ámbito estrictamente doméstico que no esté integrado o conectado a una red de difusión de cualquier tipo. A efectos de esta licencia se considerará comunicación pública la puesta a disposición del público de la obra por procedimientos alámbricos o inalámbricos, incluida la puesta a disposición del público de la obra de tal forma que cualquier persona pueda acceder a ella desde el lugar y en el momento que elija.

n. La **"explotación"** de la obra comprende su reproducción, distribución, comunicación pública y transformación.

o. Tendrán la consideración de **"bases de datos"** las colecciones de obras ajenas, de datos o de otros elementos independientes como las antologías y las bases de datos propiamente dichas que por la selección o disposición de sus contenidos constituyan creaciones intelectuales, sin perjuicio, en su caso, de los derechos que pudieran subsistir sobre dichos contenidos.

p. Los **"elementos de la licencia"** son las características principales de la licencia según la selección efectuada por el licenciador e indicadas en el título de esta licencia: Reconocimiento de autoría (Reconocimiento), Sin uso comercial (NoComercial), Compartir de manera igual (CompartirIgual).

2. Límites y uso legítimo de los derechos. Nada en esta licencia pretende reducir o restringir cualesquiera límites legales de los derechos exclusivos del titular de los derechos de propiedad intelectual de acuerdo con la Ley de Propiedad Intelectual o cualesquiera otras leyes aplicables, ya sean derivados de usos legítimos, tales como el derecho de copia privada o el derecho a cita, u otras limitaciones como la derivada de la primera venta de ejemplares.

3. Concesión de licencia. Conforme a los términos y a las condiciones de esta licencia, el licenciador concede (durante toda la vigencia de los derechos de propiedad intelectual) una licencia de ámbito mundial, sin derecho de remuneración, no exclusiva e indefinida que incluye la cesión de los siguientes derechos:

a. Derecho de reproducción, distribución y comunicación pública sobre la obra;

b. Derecho a incorporarla en una o más obras conjuntas o bases de datos y para su reproducción en tanto que incorporada a dichas obras conjuntas o bases de datos;

c. Derecho para efectuar cualquier transformación sobre la obra y crear y reproducir obras derivadas;

d. Derecho de distribución y comunicación pública de copias o grabaciones de la obra, como incorporada a obras conjuntas o bases de datos;

e. Derecho de distribución y comunicación pública de copias o grabaciones de la obra, por medio de una obra derivada.

Los anteriores derechos se pueden ejercitar en todos los medios y formatos, tangibles o intangibles, conocidos o por conocer. Los derechos mencionados incluyen el derecho a efectuar las modificaciones que sean precisas técnicamente para el ejercicio de los derechos en otros medios y formatos. Todos los derechos no cedidos expresamente por el licenciador quedan reservados, incluyendo, a título enunciativo pero no limitativo, los establecidos en la sección 4(e).

4. Restricciones. La cesión de derechos que supone esta licencia se encuentra sujeta y limitada a las restricciones siguientes:

a. Usted puede reproducir, distribuir o comunicar públicamente la obra solamente bajo términos de esta licencia y debe incluir una copia de la misma o su Identificador Uniforme de Recurso (URI), con cada copia o grabación de la obra que usted reproduzca, distribuya o comunique públicamente. Usted no puede ofrecer o imponer ningún término sobre la obra que altere o restrinja los términos de esta licencia o el ejercicio de sus derechos por parte de los cesionarios de la misma. Usted no puede sublicenciar la obra. Usted debe mantener intactos todos los avisos que se refieran a esta licencia y a la ausencia de garantías. Usted no puede reproducir, distribuir o comunicar públicamente la obra con medidas tecnológicas que controlen el acceso o uso de la obra de una manera contraria a los términos de esta licencia. Lo anterior se aplica a una obra en tanto que incorporada a una obra conjunta o base de datos, pero no implica que éstas, al margen de la obra objeto de esta licencia, tengan que estar sujetas a los términos de la misma. Si usted crea una obra conjunta o base de datos, previa comunicación del licenciador, usted deberá quitar de la obra conjunta o base de datos cualquier referencia a dicho licenciador o al autor original, según lo que se le requiera y en la medida de lo posible. Si usted crea una obra derivada, previa comunicación del licenciador, usted deberá quitar de la obra derivada cualquier referencia a dicho licenciador o al autor original, lo que se le requiera y en la medida de lo posible.

b. Usted puede reproducir, distribuir o comunicar públicamente una obra derivada solamente bajo los términos de esta licencia o de una versión posterior de esta licencia con sus mismos elementos principales o de una licencia iCommons de Creative Commons que contenga los mismos elementos principales que esta licencia (ejemplo: Reconocimiento-NoComercial-Compartir 2.0 Japón). Usted debe incluir una copia de la esta licencia o de la mencionada anteriormente o bien su Identificador Uniforme de Recurso (URI), con cada copia o grabación de la obra que usted reproduzca, distribuya o comunique públicamente. Usted no puede ofrecer o imponer ningún término respecto de las obras derivadas o sus transformaciones que alteren o restrinjan los términos de esta licencia o el ejercicio de sus derechos por parte de los cesionarios de la misma, Usted debe mantener intactos todos los avisos que se refieran a esta licencia y a la ausencia de garantías. Usted no puede reproducir, distribuir o comunicar públicamente la obra derivada con medidas tecnológicas que controlen el acceso o uso de la obra de una manera contraria a los términos de esta licencia. Lo anterior se aplica a una obra derivada en tanto que incorporada a una obra conjunta o base de datos, pero no implica que éstas, al margen de la obra objeto de esta licencia, tengan que estar sujetas a los términos de esta licencia.

c. Usted no puede ejercitar ninguno de los derechos cedidos en la sección 3 anterior de manera que pretenda principalmente o se encuentre dirigida hacia la obtención de un beneficio mercantil o la remuneración monetaria privada. El intercambio de la obra por otras obras protegidas por la propiedad intelectual mediante sistemas de compartir archivos no se considerará como una manera que pretenda principalmente o se encuentre dirigida hacia la obtención de un beneficio mercantil o la remuneración monetaria privada, siempre que no haya ningún pago de cualquier remuneración monetaria en relación con el intercambio de las obras protegidas.

d. Si usted reproduce, distribuye o comunica públicamente la obra o cualquier obra derivada, conjunta o base datos que la incorpore, usted debe mantener intactos todos los avisos sobre la propiedad intelectual de la obra y reconocer al autor original, de manera razonable conforme al medio o a los medios que usted esté utilizando, indicando el nombre (o el seudónimo, en su caso) del autor original si es facilitado; el título de la obra si es facilitado; de manera razonable, el Identificador Uniforme de Recurso (URI), si existe, que el licenciador especifica para ser vinculado a la obra, a menos que tal URI no se refiera al aviso sobre propiedad intelectual o a la información sobre la licencia de la obra; y en el caso de una obra derivada, un aviso que identifique el uso de la obra en la obra derivada (e.g., "traducción francesa de la obra de Autor Original," o "guión basado en obra original de Autor Original"). Tal aviso se puede desarrollar de cualquier manera razonable; con tal de que, sin embargo, en el caso de una obra derivada, conjunta o base datos, aparezca como mínimo este aviso allá donde aparezcan los avisos correspondientes a otros autores y de forma comparable a los mismos.

e. Para evitar la duda, sin perjuicio de la preceptiva autorización del licenciador y especialmente cuando la obra se trate de una obra audiovisual, el licenciador se reserva el derecho exclusivo a percibir, tanto individualmente como mediante una entidad de gestión de derechos o varias, (por ejemplo: SGAE, Dama, VEGAP), los derechos de explotación de la obra, así como los derivados de obras derivadas, conjuntas o bases de datos, si dicha explotación pretende principalmente o se encuentra dirigida hacia la obtención de un beneficio mercantil o la remuneración monetaria privada.

f. En el caso de la inclusión de la obra en alguna base de datos o recopilación, el propietario o el gestor de la base de datos deberá renunciar a cualquier derecho relacionado con esta inclusión y concerniente a los usos de la obra una vez extraída de las bases de datos, ya sea de manera individual o conjuntamente con otros materiales.

5. Exoneración de responsabilidad

A MENOS QUE SE ACUERDE MUTUAMENTE ENTRE LAS PARTES, EL LICENCIADOR OFRECE LA OBRA TAL CUAL (ON AN "AS-IS" BASIS) Y NO CONFIERE NINGUNA GARANTÍA DE CUALQUIER TIPO RESPECTO DE LA OBRA O DE LA PRESENCIA O AUSENCIA DE ERRORES QUE PUEDAN O NO SER DESCUBIERTOS. ALGUNAS JURISDICCIONES NO PERMITEN LA EXCLUSIÓN DE TALES GARANTÍAS, POR LO QUE TAL EXCLUSIÓN PUEDE NO SER DE APLICACIÓN A USTED.

6. Limitación de responsabilidad.

SALVO QUE LO DISPONGA EXPRESA E IMPERATIVAMENTE LA LEY APLICABLE, EN NINGÚN CASO EL LICENCIADOR SERÁ RESPONSABLE ANTE USTED POR CUALQUIER TEORÍA LEGAL DE CUALESQUIERA DAÑOS RESULTANTES, GENERALES O ESPECIALES (INCLUIDO EL DAÑO EMERGENTE Y EL LUCRO CESANTE), FORTUITOS O CAUSALES, DIRECTOS O INDIRECTOS, PRODUCIDOS EN CONEXIÓN CON ESTA LICENCIA O EL USO DE LA OBRA, INCLUSO SI EL LICENCIADOR HUBIERA SIDO INFORMADO DE LA POSIBILIDAD DE TALES DAÑOS.

7. Finalización de la licencia

a. Esta licencia y la cesión de los derechos que contiene terminarán automáticamente en caso de cualquier incumplimiento de los términos de la misma. Las personas o entidades que hayan recibido obras derivadas, conjuntas o bases de datos de usted bajo esta licencia, sin embargo, no verán sus licencias finalizadas, siempre que tales personas o entidades se mantengan en el cumplimiento íntegro de esta licencia. Las secciones 1, 2, 5, 6, 7 y 8 permanecerán vigentes pese a cualquier finalización de esta licencia.

b. Conforme a las condiciones y términos anteriores, la cesión de derechos de esta licencia es perpetua (durante toda la vigencia de los derechos de propiedad intelectual aplicables a la obra). A pesar de lo anterior, el licenciador se reserva el derecho a divulgar o publicar la obra en condiciones distintas a las presentes o de retirar la obra en cualquier momento. No obstante, ello no supondrá dar por concluida esta licencia (o cualquier otra licencia que haya sido concedida o sea necesario ser concedida, bajo los términos de esta licencia), que continuará vigente y con efectos completos a no ser que haya finalizado conforme a lo establecido anteriormente.

8. Miscelánea

a. Cada vez que usted explote de alguna forma la obra o una obra conjunta o una base datos que la incorpore, el licenciador original ofrece a los terceros y sucesivos licenciatarios la cesión de derechos sobre la obra en las mismas condiciones y términos que la licencia concedida a usted.

b. Cada vez que usted explote de alguna forma una obra derivada, el licenciador original ofrece a los terceros y sucesivos licenciatarios la cesión de derechos sobre la obra original en las mismas condiciones y términos que la licencia concedida a usted.

c. Si alguna disposición de esta licencia resulta inválida o inaplicable según la Ley vigente, ello no afectará la validez o aplicabilidad del resto de los términos de esta licencia y, sin ninguna acción adicional por cualquiera las partes de este acuerdo, tal disposición se entenderá reformada en lo estrictamente necesario para hacer que tal disposición sea válida y ejecutiva.

d. No se entenderá que existe renuncia respecto de algún término o disposición de esta licencia, ni que se consiente violación alguna de la misma, a menos que tal renuncia o consentimiento figure por escrito y lleve la firma de la parte que renuncie o consienta.

e. Esta licencia constituye el acuerdo pleno entre las partes con respecto a la obra objeto de la licencia. No caben interpretaciones, acuerdos o términos con respecto a la obra que no se encuentren expresamente especificados en la presente licencia. El licenciador no estará obligado por ninguna disposición complementaria que pueda aparecer en cualquier comunicación de usted. Esta licencia no se puede modificar sin el mutuo acuerdo por escrito entre el licenciador y usted.

Creative Commons no es parte de esta licencia y no ofrece ninguna garantía en relación con la obra. Creative Commons no será responsable frente a usted o a cualquier parte, por cualquier teoría legal de cualesquiera daños resultantes, incluyendo, pero no limitado, daños generales o especiales (incluido el daño emergente y el lucro cesante), fortuitos o causales, en conexión con esta licencia. A pesar de las dos (2) oraciones anteriores, si Creative Commons se ha identificado expresamente como el licenciador, tendrá todos los derechos y obligaciones del licenciador.

Salvo para el propósito limitado de indicar al público que la obra está licenciada bajo la CCPL, ninguna parte utilizará la marca registrada "Creative Commons" o cualquier marca registrada o insignia relacionada con "Creative Commons" sin su consentimiento por escrito. Cualquier uso permitido se hará de conformidad con las pautas vigentes en cada momento sobre el uso de la marca registrada por "Creative Commons", en tanto que sean publicadas su página web (website) o sean proporcionadas a petición previa.

Puede contactar con Creative Commons en: http://creativecommons.org/.

Otras notas acerca de esta publicación.

La información contenida en este manual se distribuye con la esperanza de que sea de utilidad y se proporciona tal cual es pero **SIN GARANTÌA ALGUNA**, aún sin la garantía implícita de comercialización o adecuamiento para un propósito en particular y el autor o autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de esta.

Linux® es una marca registrada de Linus Torvalds, Red Hat™ Linux, RPM® y GLINT® son marcas registradas de Red Hat Software, Unix® es marca registrada de X/Open. MS-DOS®, MS-Office® y Windows® son marcas registradas de Microsoft Corporation. X Window System® es marca registrada de X Consortium, Inc., TrueType es una marca registrada de Apple Computer, WordPerfect® es una marca registrada de Corel Corporation, StarOffice® es una marca registrada de Sun Mycrosystems. Apache® es una marca registrada de The Apache Group. Fetchmail® es una marca registrada de Eric S. Raymond. Sendmail® es una marca registrada de Sendmail, Inc. Darkshram™ es ©1987 y marca registrada de Joel Barrios Dueñas.

1. ¿Que es GNU/Linux?

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

GNU es un acrónimo recursivo que significa **GNU No es Unix** (**G**NU is **N**ot **U**nix). Este proyecto fue iniciado por **Richard Stallman** y anunciado el 27 de septiembre de 1983, con el objetivo de crear un sistema operativo completamente libre.

GNU/Linux® es un poderoso y sumamente versátil sistema operativo con licencia libre y que implemente el estándar **POSIX** (acrónimo de **P**ortable **O**perating **S**ystem **I**nterface, que se traduce como Interfaz de Sistema Operativo Portable). Fue creado en 1991 por **Linus Torvalds**, siendo entonces un estudiante de la Universidad de Helsinski, Finlandia. En 1992, el núcleo **Linux**> fue combinado con el sistema **GNU**. El Sistema Operativo formado por esta combinación se conoce como **GNU/Linux**.

GNU/Linux es **equipamiento lógico libre** o *Software Libre*. Esto significa que el usuario tiene la libertad de redistribuir y modificar a de acuerdo a necesidades específicas, siempre que se incluya el código fuente, como lo indica la Licencia Pública General GNU (acrónimo de **G**NU is **N**ot **U**nix), que es el modo que ha dispuesto la Free Software Foundation (Fundación de equipamiento lógico libre). Esto también incluye el derecho a poder instalar el núcleo de **GNU/Linux®** en cualquier número de ordenadores o equipos de cómputo que el usuario desee.

GNU/Linux® **no es equipamiento lógico gratuito** (comúnmente denominado como Freeware), se trata de **equipamiento lógico libre** o *Software Libre*. Cuando nos referirnos a *libre*, lo hacemos en relación a la libertad y no al precio. La **GPL** (acrónimo de **G**eneral **P**ublic **L**icence, que se traduce como Licencia Pública General), a la cual Linus Torvalds incorporó a Linux, está diseñada para asegurar que el usuario tenga siempre la libertad de distribuir copias del equipamiento lógico (y cobrar por el servicio si así lo desea). La **GPL** tiene como objetivo garantizar al usuario la libertad de compartir y cambiar **equipamiento lógico libre**, es decir, asegurarse de que el equipamiento lógico siempre permanezca libre para todos los usuarios. La **GPL** es aplicable a la mayoría del equipamiento lógico de la Free Software Foundation así como a cualquier otro programa cuyos autores se comprometan a usarlo.

GNU/Linux® es también de la mejor alternativa de siglo XXI para los usuarios que no solo desean libertad, sino que también desean un sistema operativo estable, robusto y confiable. Es un sistema operativo idóneo para utilizar en Redes, como es el caso de servidores, estaciones de trabajo y **también** para computadoras personales.

Las características de GNU/Linux® le permiten desempeñar múltiples tareas en forma simultánea de forma segura y confiable. Los distintos servicios servicios se pueden detener, iniciar o reiniciar independientemente sin afectar al resto del sistema permitiendo operar las 24 horas del día los 365 días del año.

Tal ha sido el impacto alcanzado por GNU/Linux® en los últimos años, que muchas de las empresas de Software más importantes del mundo, entre las cuales están IBM, Oracle y Sun Microsystems, han encontrado en GNU/Linux una plataforma con un muy amplio mercado y se han volcado al desarrollo de versiones para Linux de sus más importantes aplicaciones. Grandes corporaciones, como Compaq, Dell, Hewlett Packard, IBM y muchos más, llevan varios años distribuyendo equipos con GNU/Linux® como sistema operativo.

Gracias a sus características, la constante evolución de los ambientes gráficos para X Window®, que cada vez son de más fácil uso, como es el caso de GNOME y KDE, al trabajo de cientos de programadores y usuarios fieles alrededor del mundo, Linux ha dejado de ser un sistema operativo poco atractivo y complicado de utilizar para convertirse en una alternativa real para quienes buscan un sistema operativo confiable y poderoso, ya sea para una servidor, estación de trabajo o la computadora personal de un usuario intrépido.

1.1. Requerimientos del sistema

Se debe contar con la suficiente cantidad de memoria y un microprocesador en buen estado. Con casi cualquier distribución comercial de Linux, el ambiente gráfico necesitará al menos 640 MB RAM y 1 GB de espacio libre en disco duro para la instalación mínima. Para contar con una cantidad mínima de aplicaciones, se requieren al menos 2 GB adicionales de espacio libre en disco duro, repartido en al menos 3 particiones. Se recomienda como mínimo un microprocesador i686 a 1 GHz. Sin ambiente gráfico, como es el caso de un servidor o bien solamente aplicaciones para modo de texto, se requieren al menos 384 MB RAM y un microprocesador i686 a 500 MHz serán suficientes.

El servidor de vídeo puede funcionar con sólo 128 MB RAM; pero su desempeño será **extremadamente lento**. Algunas aplicaciones para modo gráfico pueden necesitar escalar 256 MB, 512 MB o 1 GB de RAM adicional. El mínimo recomendado para utilizar GNOME 2.x es de 384 MB RAM; se recomiendan 512 MB. El óptimo es de 1 GB RAM.

Si desea instalar Linux en una computadora personal con las suficientes aplicaciones para ser totalmente funcional y productivo y contar con el espacio necesario para instalar herramientas de oficina (OpenOffice.org), se **recomienda** contar con al menos 4 GB de espacio libre en disco, al menos 512 MB RAM y un microprocesador i686, a cuando menos 1 GHz.

El instalador en modo texto de **CentOS 6** y **Red Hat Enterprise Linux 6** requiere al menos 384 MB RAM., mientras que el instalador en modo gráfico de éstos requeire al menos 640 MB RAM.

2. Estándar de Jerarquía de Sistema de Archivos

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Artículo basado sobre el publicado en inglés por Wikipedia, Enciclopedia Libre, en http://en.wikipedia.org/wiki/FHS.

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

2.1. Introducción.

El estándar de jerarquía de archivos (**FHS** o **F**ilesystem **H**ierarchy **S**tandard) define los principales directorios y sus contenidos en GNU/Linux y otros sistemas operativos similares a Unix.

En agosto de 1993 inició el proceso para desarrollar un estándar de sistema de archivos jerárquico, como un esfuerzo para reorganizar la estructuras de archivos y directorios de GNU/Linux. El 14 de Febrero de 1994 se publicó el **FSSTND** (**F**ile**s**ystem **St**a**nd**ard), un estándar de jerarquía de archivos específico para GNU/Linux. Revisiones de éste se publicaron el 9 de Octubre de 1994 y el 28 de Marzo de 1995.

A principios de 1996, con la ayuda de miembros de la comunidad de desarrolladores de BSD, se fijó como objetivo el desarrollar una versión de **FSSTND** más detallada y dirigida no solo hacia Linux sino también hacia otros sistemas operativos similares a Unix. Como uno de los resultados el estándar cambió de nombre a **FHS** o **F**ilesystem **H**ierarchy **S**tandard.

El **FHS** es mantenido por **Free Standards Group**, una organización sin fines de lucro constituida por compañías que manufacturan sustento físico (*Hardware*) y equipamiento lógico (*Software*) como Hewlett Packard, Dell, IBM y Red Hat. La mayoría de las distribuciones de Linux, inclusive las que forman parte de Free Software Standards, utilizan este estándar sin aplicarlo de manera estricta.

La versión 2.3 del FHS, que es la utilizada por **CentOS**, **Fedora™**, **Red Hat™ Enterprise Linux**, **openSUSE™** y **SUSE™ Linux Enterprise**, fue anunciada el 29 de enero de 2004.

2.2. Estructura de directorios.

Todos los archivos y directorios aparecen debajo del directorio raíz «/», aún si están almacenados en dispositivos físicamente diferentes.

Directorio.	Descripción
/bin/	Mandatos binarios esenciales (como son cp, mv, ls, rm, mkdir, etc.),
/boot/	Archivos utilizados durante el inicio del sistema (núcleo y discos RAM),
/dev/	Dispositivos esenciales,
/etc/	Archivos de configuración utilizados en todo el sistema y que son específicos del anfitrión.
/etc/opt/	Archivos de configuración utilizados por programas alojados dentro de /opt/
/etc/X11/ (opcional)	Archivos de configuración para el sistema X Window.
/etc/sgml/ (opcional)	Archivos de configuración para SGML.
/etc/xml/ (opcional)	Archivos de configuración para XML.

Directorio.	Descripción
/home/ (opcional)	Directorios de inicio de los usuarios locales.
/lib/ y /lib64/	Bibliotecas compartidas esenciales para los binarios de /bin/, /sbin/ y el núcleo del sistema. /lib64/ corresponde al directorio utilizado por sistemas de 64-bit.
/mnt/	Sistemas de archivos montados temporalmente.
/media/	Puntos de montaje para dispositivos de medios, como son las unidades lectoras de discos compactos.
/opt/	Paquetes de aplicaciones de terceros.
/proc/	Sistema de archivos virtual que documenta sucesos y estados del núcleo. Contiene, principalmente, archivos de texto.
/root/ (opcional)	Directorio de inicio del usuario root (super-usuario).
/sbin/	Binarios de administración de sistema.
/tmp/	Archivos temporales
/srv/	Datos específicos de sitio, servidos por el sistema.

Directorio.	Descripción
/usr/	Jerarquía secundaria para datos compartidos de solo lectura (**U**nix **s**ystem **r**esources). Este directorio debe poder ser compartido para múltiples anfitriones, y, debe evitarse que contenga datos específicos del anfitrión que los comparte cuando se hace a través de NFS.
/usr/bin/	Mandatos binarios.
/usr/include/	Archivos de inclusión estándar (cabeceras de desarrollo).
/usr/lib/ y /usr/lib64	Bibliotecas compartidas. /usr/lib64/ corresponde al directorio utilizado por sistemas de 64-bit.
/usr/share/	Datos compartidos, independientes de la arquitectura del sistema. Consiste en imágenes, archivos de texto, archivos de audio, etc.
/usr/src/ (opcional)	Códigos fuente.
/usr/X11R6/ (opcional)	Sistema X Window, versión 11, lanzamiento 6. Prácticamente ninguna distribución de Linux lo utiliza en la actualidad.
/usr/local/	Jerarquía terciaria para datos compartidos de solo-lectura, específicos del anfitrión.

Directorio.	Descripción
/var/	Archivos variables, como son bitácoras, bases de datos, directorio raíz de servidores HTTP y FTP, colas de correo, archivos temporales, etc.
/var/account/ (opcional)	Procesa bitácoras de cuentas de usuarios.
/var/cache/	Cache da datos de aplicaciones.
/var/crash/ (opcional)	Depósito de información referente a fallas del sistema.
/var/games/ (opcional)	Datos variables de aplicaciones para juegos.
/var/lib/	Información de estado variable. Algunos servidores como MySQL y PostgreSQL, almacenan sus bases de datos en directorios subordinados de éste.
/var/lock/	Archivos de bloqueo de los servicios en ejecución.
/var/log/	Archivos y directorios, utilizados para almacenar las bitácoras de eventos del sistema.
/var/mail/ (opcional)	Buzones de correo de usuarios.
/var/opt/	Datos variables de /opt/.
/var/spool/	Colas de procesamiento y carretes de datos de aplicaciones.
/var/tmp/	Archivos temporales que prevalecen después de un reinicio.

Más detalles acerca del **FHS** en http://www.pathname.com/fhs/.

2.3. Particiones recomendadas para instalar CentOS, Fedora™, Red Hat™ Enterprise Linux, openSUSE™ y SUSE™ Linux Enterprise.

Si las condiciones limitan el número de particiones a utilizar, como mínimo se requieren dos particiones (diseño predeterminado de **openSUSE™** y **SUSE™ Linux Enterprise**):

/	Asignar todo el espacio disponible de la unidad de almacenamiento.
Swap	Si se tiene menos de 1 GiB de RAM, se debe asignar el **doble del tamaño del RAM físico**; si se tiene más de 1 GiB RAM, se debe asignar una cantidad igual al tamaño del RAM físico, más 2 GiB. Ésta será siempre la última partición del espacio disponible para almacenamiento y jamás se le asigna punto de montaje.

Para uso general, se recomienda utilizar un diseño de tres particiones (predeterminado del instalador de **CentOS**, **Fedora™** y **Red Hat™ Enterprise Linux**):

/boot	Requiere de 200 MiB a 512 MiB.
/	Si se utiliza el diseño de tres particiones, asignar el resto del espacio disponible en la unidad de almacenamiento. Si se van asignar particiones para los directorios mencionados adelante, se requieren de 3072 MiB a 5120 MiB.
Swap	Si se tiene menos de 1 GiB de RAM, se debe asignar el **doble del tamaño del RAM físico**; si se tiene más de 1 GiB RAM, se debe asignar una cantidad igual al tamaño del RAM físico, más 2 GiB. Ésta será siempre la última partición del espacio disponible para almacenamiento y jamás se le asigna punto de montaje.

Lo siguientes directorios jamás deberán estar fuera de la partición que corresponda a **/**, es decir, **jamás se deben asignar como particiones separadas**:

- /etc
- /bin
- /dev
- /lib y /lib64
- /media
- /mnt

- /proc
- /root
- /sbin
- /sys

Para futuras versiones de **CentOS**, **Fedora™**, **Red Hat™ Enterprise Linux**, **openSUSE™** y **SUSE™ Linux Enterprise**, el directorio **/var** también deberá estar dentro de la misma partición que corresponda a **/**, pues el proceso de arranque, que será gestionado por **Systemd**, así lo requerirá.

Otras particiones que se recomienda asignar, son:

`/usr`	Requiere al menos 3072 MiB en instalaciones básicas. Debe considerarse el equipamiento lógico se planee instalar a futuro. Para uso general se recomiendan al menos de 5120 MiB, y, de ser posible, considere un tamaño óptimo de hasta 20480 MiB.
`/tmp`	Requiere al menos 350 MiB y puede asignarse hasta 5 GiB o más, dependiendo de la carga de trabajo y del tipo de aplicaciones. Si, por ejemplo, el sistema cuenta con un grabador de DVD, será necesario asignar a /tmp el espacio suficiente para almacenar una imagen de disco DVD, es decir, al menos 4.2 GiB, asumiendo que es de una sola cara y de densidad simple.
`/var`	Requiere **al menos** 3072 MiB en estaciones de trabajo **sin servicios**. En servidores regularmente se le asigna **al menos la mitad del espacio disponible para almacenamiento**.
`/home`	En estaciones de trabajo, a esta partición se asigna al menos la mitad del espacio disponible para almacenamiento.
`/usr/local`	Requiere al menos 3072 MiB en instalaciones básicas. Debe considerarse el equipamiento lógico que se planee compilar desde código fuente, e instalar, a futuro. Al igual que `/usr`, para uso general se recomiendan al menos de 5120 MiB, y, de ser posible, considere un tamaño óptimo de hasta 20480 MiB.
`/opt`	Requiere al menos 3072 MiB en instalaciones básicas. Debe considerarse el equipamiento lógico de terceros que se planee instalar a futuro. Al igual que `/usr`, para uso general se recomiendan al menos de 5120 MiB, y, de ser posible, considere un tamaño óptimo de hasta 20480 MiB.
`/var/lib`	Si se asigna como partición independiente de `/var`, lo cual permitiría optimizar el registro por diario utilizando el modo *journal* para un mejor desempeño, requiere al menos 3072 MiB en instalaciones básicas. Deben considerarse las bases de datos o directorios de LDAP, que se planeen hospedar a futuro.
`/var/www`	Si se asigna como partición independiente de `/var`, lo cual permitiría optimizar el registro por diario utilizando el modo *writeback* para un mejor desempeño, requiere al menos 3072 MiB en instalaciones básicas. Deben considerarse los anfitriones virtuales, aplicaciones y contenido para ser servido a través del protocolo HTTP, que se planeen hospedar a futuro.

2.4. Bibliografía.

- secure.wikimedia.org/wikipedia/en/wiki/Filesystem_Hierarchy_Standard

3. Procedimiento de instalación de CentOS 6.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

3.1. Procedimientos.

3.1.1. Planeación.

Antes de comenzar, determine primero los siguientes puntos:

- **Finalidad productiva**. ¿Va ser un servidor, estación de trabajo o escritorio? ¿Qué uso va tener el equipo? ¿Qué servicios va a requerir? Idealmente lo que se establezca en este punto debe prevalecer sin modificaciones a lo largo de su ciclo productivo.
- **Ciclo de producción**. ¿Cuánto tiempo considera que estará en operación el equipo? ¿Seis meses, un año, dos años, cinco años?
- **Capacidad del equipo**. ¿A cuántos usuarios simultáneos se brindará servicio? ¿Tiene el equipo la cantidad suficiente de RAM y poder de procesamiento suficiente?
- **Particiones del disco duro**. Determine cómo administrará el espacio disponible de almacenamiento. Para más detalles al respecto, consulte el documento titulado «**Estándar de Jerarquía de Sistema de Archivos**.»
- **Limitaciones**. Tenga claro que **CentOS** —al igual que sucede con **Red Hat Enterprise Linux** — es un sistema operativo diseñado y enfocado específicamente para ser utilizado como sistema operativo en servidores, desarrollo de programas y estaciones de trabajo. Salvo que posteriormente se añada algún almacén YUM como EPEL, Remi, AL Server o RPMFusion, este sistema operativo carecerá de soporte para medios de audio y video en formatos privativos — como ocurre son el soporte para MP3, DivX, H.264, MPEG, etc.— y que sólo incluye *Software Libre* que se encuentre exento de problemas de patentes.

Obtención de los medios.

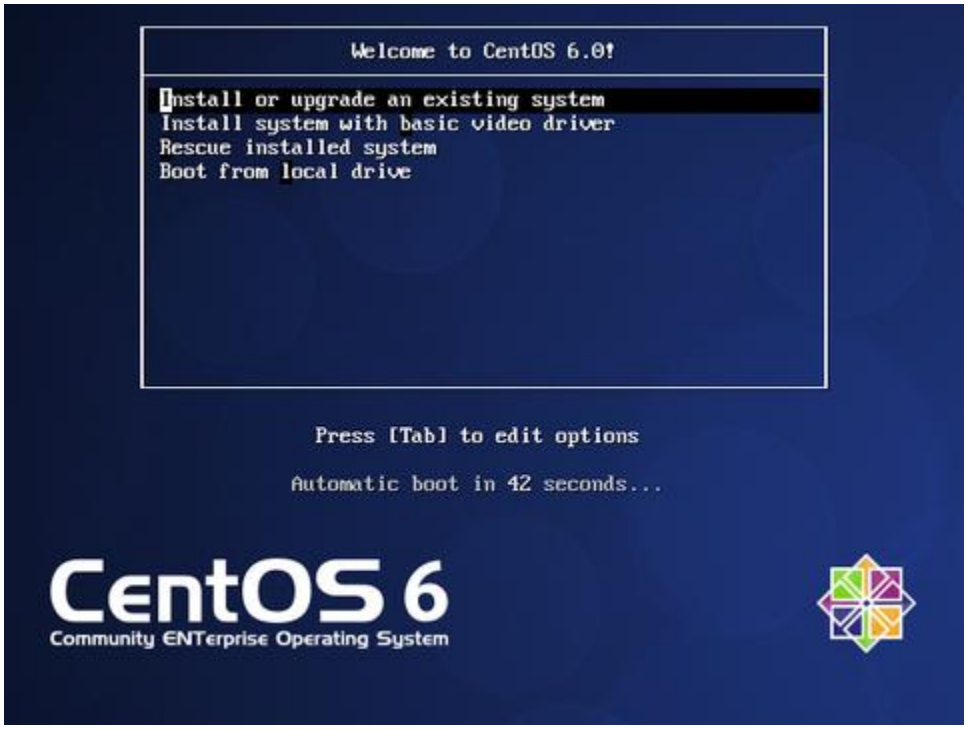
Descargue la imagen ISO del DVD de **CentOS 6** para arquitectura i386 o bien arquitectura x86-64 (sólo es necesario el DVD 1 —salvo que requiera soporte para algún idioma exótico— desde algunos de los sitios espejo que encontrará en el siguiente URL:

- http://mirror.centos.org/centos/6/isos/

Si por algún motivo en particular requiere descargar la imagen ISO del primer disco DVD de **CentOS 6.0** para arquitectura i386, **en lugar de descargar la correspondiente para CentOS 6.3**, grabe ésta en un disco virgen **DVD-R** (capacidad de 4,707,319,808 bytes). La imagen de DVD para i386 (4,705,456,128 bytes) es demasiado grande para poder ser grabada en un **DVD+R** (capacidad de 4,700,372,992 bytes). Las imágenes de los dos DVD para arquitectura x86-64, 4,238,800,896 bytes y 1,182,699,520 bytes, respectivamente, caben perfectamente en discos **DVD+R** y **DVD-R**.

3.1.2. Instalación del sistema operativo.

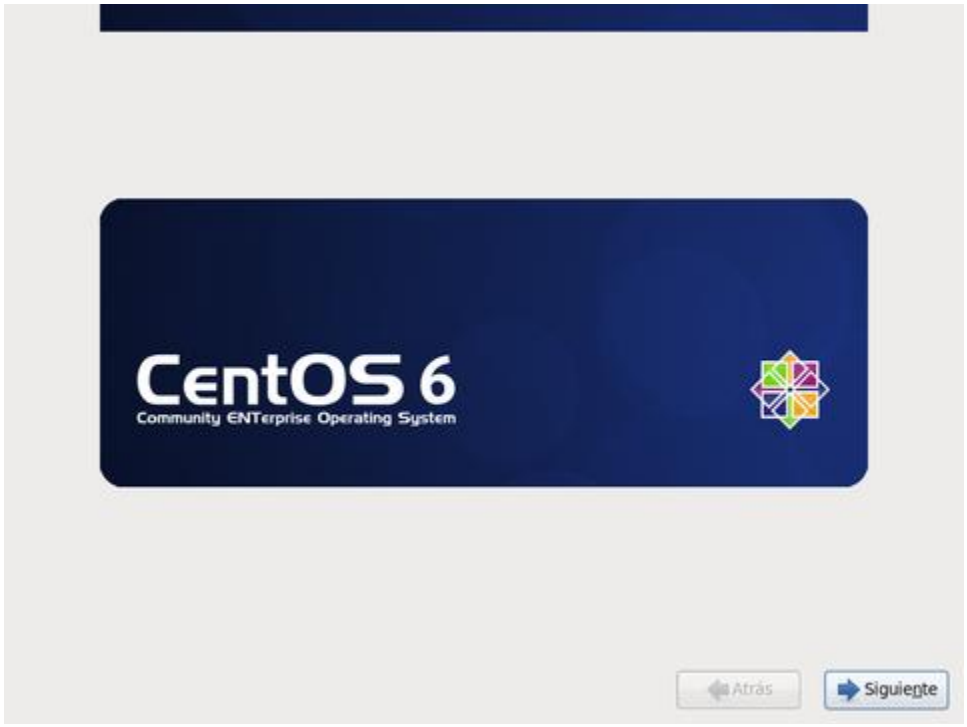
Inserte el **disco DVD** de instalación de **CentOS 6** y espere 60 segundos para el inicio automático o bien pulse la tecla **ENTER** para iniciar de manera inmediata o bien pulse la tecla **«TAB»** e ingrese las opciones de instalación deseadas.



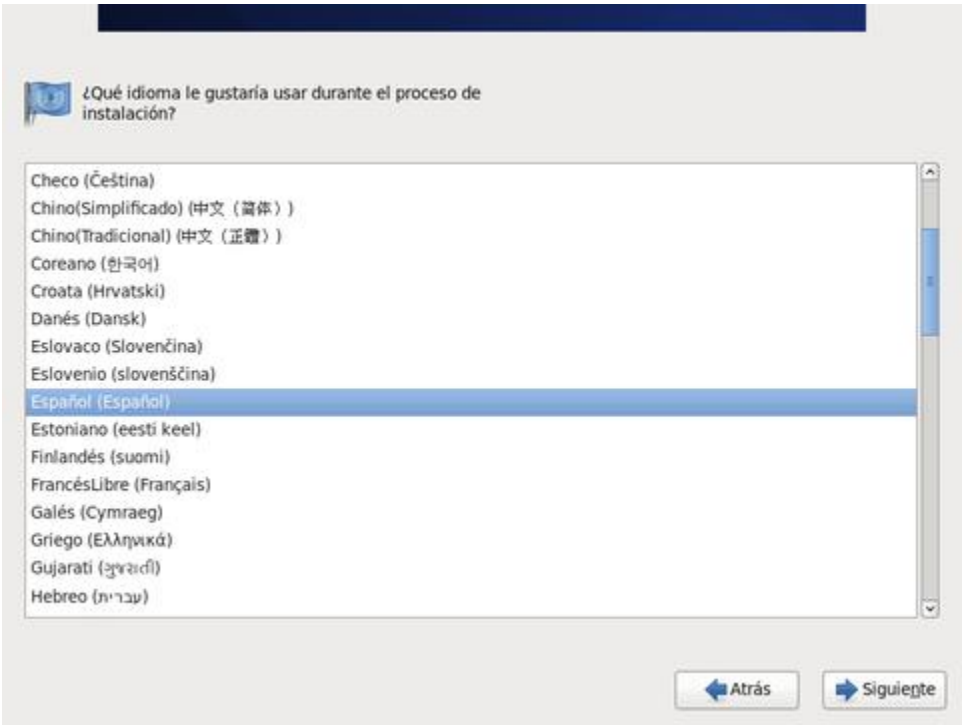
La primer pantalla que aparecerá le preguntará si desea verificar la integridad del medio de instalación. Si descargó una imagen ISO desde Internet y la grabó en un disco compacto o DVD, es buena idea verificar medios de instalación. Si está haciendo la instalación desde una máquina virtual con una imagen ISO y la suma MD5 coincide, descarte verificar.

Si desea verificar la integridad del medio de instalación (DVD o conjunto de discos compactos), a partir del cual se realizará la instalación, seleccione **«OK»** y pulse la tecla **ENTER**, considere que esto puede demorar varios minutos. Si está seguro de que el(los) disco(s) está(n) en buen estado, pulse la tecla **«TAB»** para seleccionar **«Skip»** y pulse la tecla **ENTER**.

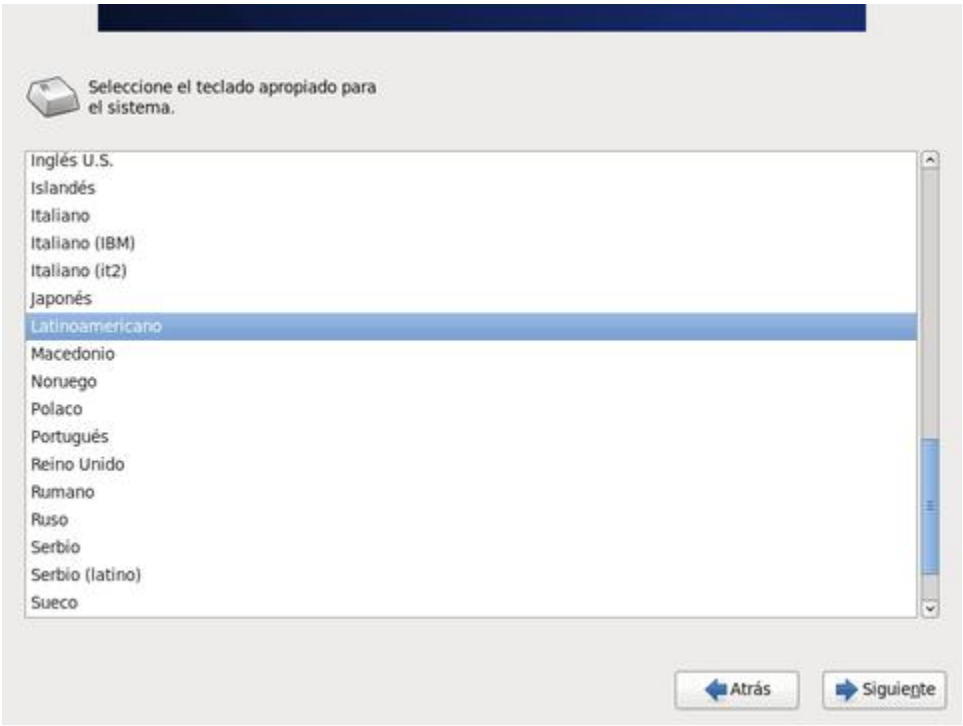
Haga clic sobre el botón **«Next»** o bien **«Siguiente»**, en cuanto aparezca la pantalla de bienvenida de CentOS.



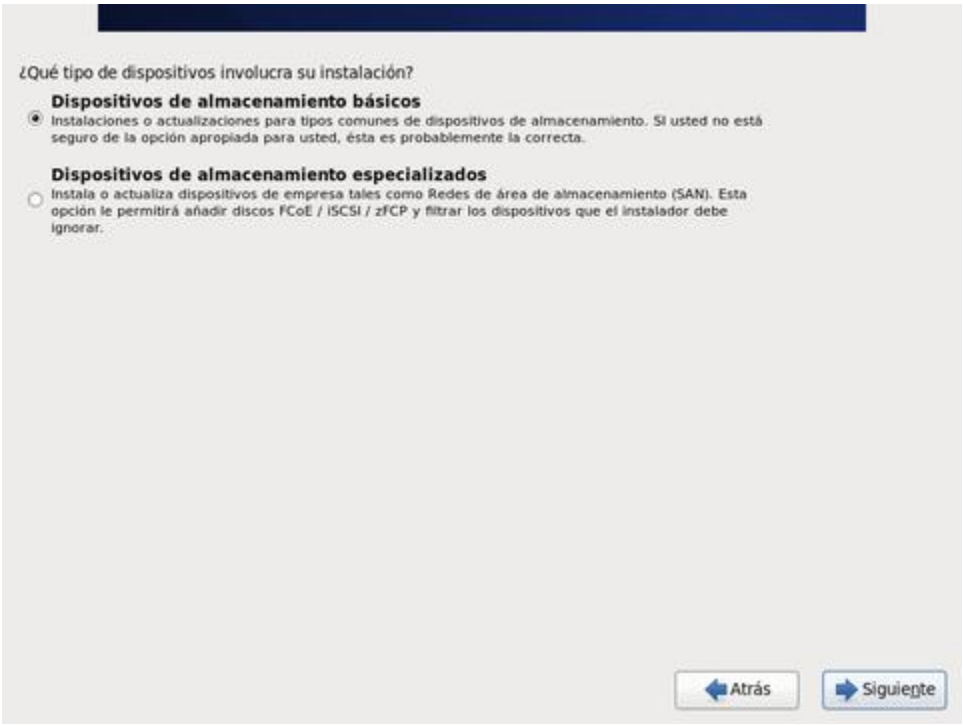
Seleccione **«Spanish»** o bien **«Español»**, como idioma para ser utilizado durante la instalación.



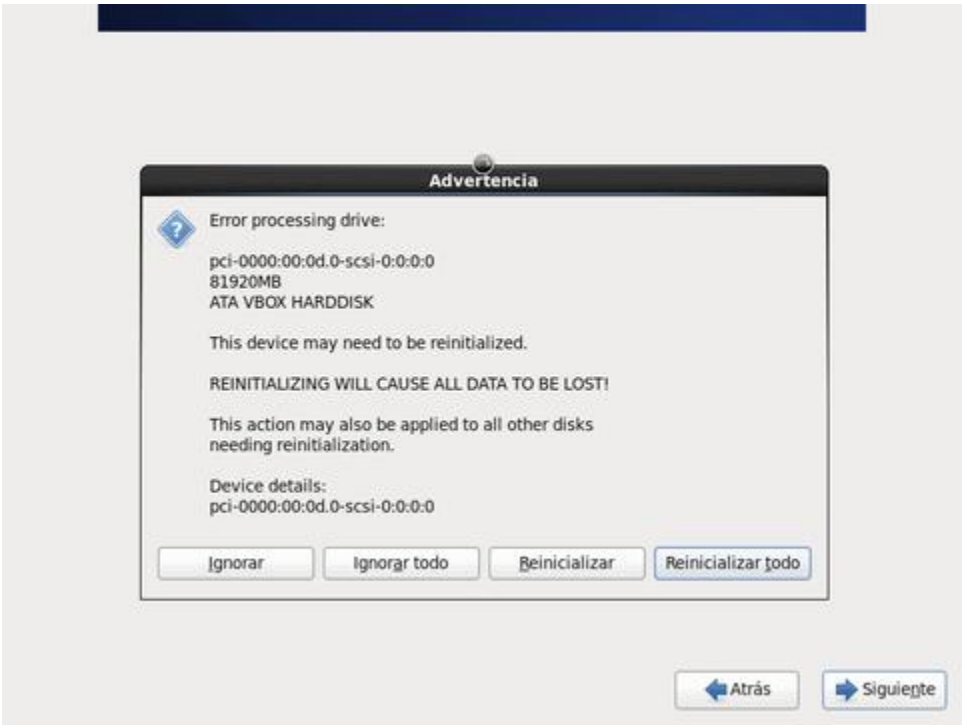
A partir de este punto, todos los textos deberán aparecer al español. Seleccione el mapa de teclado. Elija el mapa de teclado al **«Español»** o bien el mapa de teclado **«Latinoamericano»**, de acuerdo a lo que corresponda. Al terminar, haga clic sobre el botón denominado **«Siguiente.»**



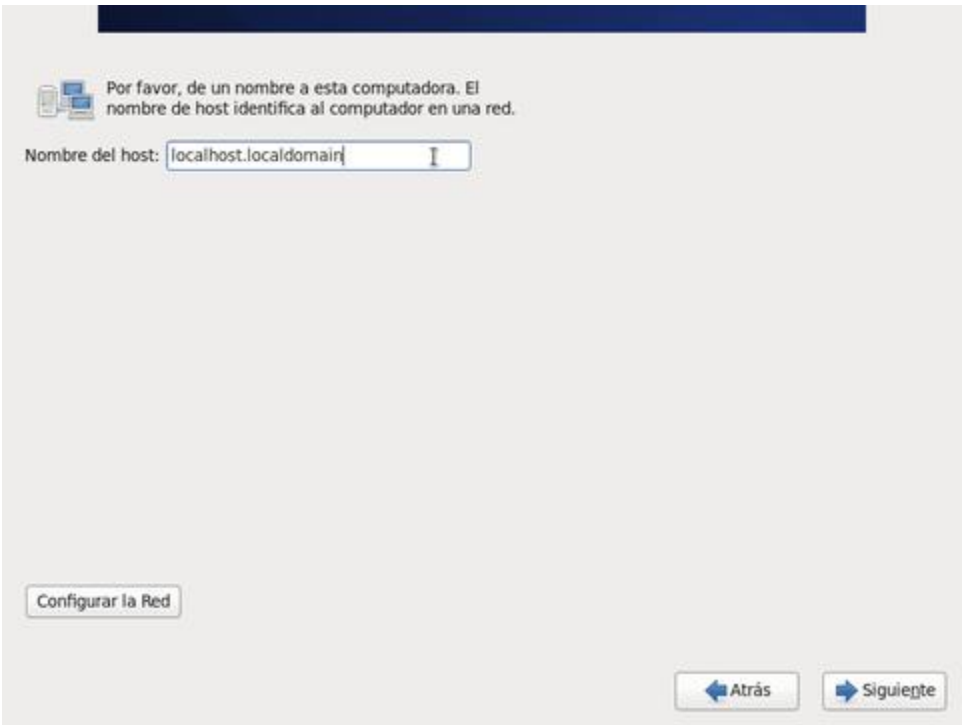
CentOS 6 incluye soporte para realizar una instalación sobre dispositivos de almacenamiento especializados, como Redes de Área de Almacenamiento (SAN), como FCoE, iSCSI y zFCP. Obviamente requiere disponer de un SAN en la red de área local para poder hacer uso de este tipo de dispositivos de almacenamiento. Si sólo dispone de discos duros en el equipo donde se realizará la instalación, elija la opción predeterminada, es decir **«Dispositivos de almacenamiento básicos»** y haga clic sobre el botón denominado **«Siguiente.»**



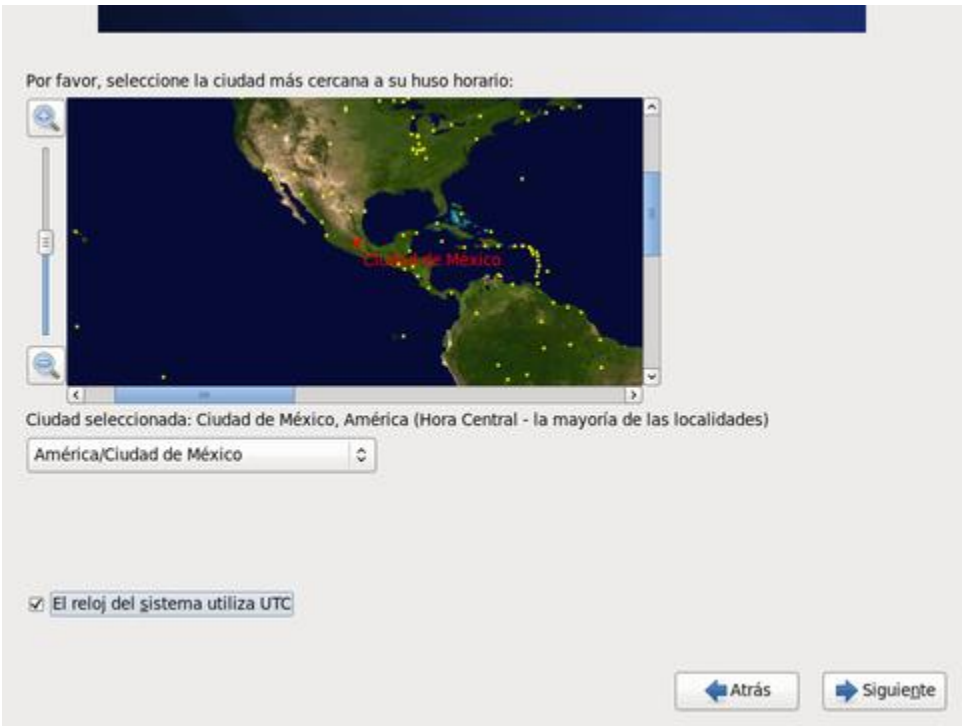
Si se trata de una unidad de almacenamiento **nueva**, es decir que carece de tabla de particiones, recibirá una advertencia respecto de que esta unidad de almacenamiento deberá ser *inicializada antes de guardar la tabla de particiones que será creada posteriormente. Si está seguro de que se trata de una unidad de almacenamiento nueva o bien a ésta le fue previamente borrada la tabla de particiones, haga clic sobre el botón* ***«Reinicializar todo.»***



Defina el nombre de anfitrión en el siguiente el formato: **nombre.dominio.tld**. Procure que el nombre de anfitrión sea corto, de hasta a 12 caracteres más el dominio y que esté resuelto en un servidor DNS. Si está indeciso al respecto, deje el valor predeterminado como **localhost.localdomain** y haga clic sobre el botón denominado **«Siguiente.»**



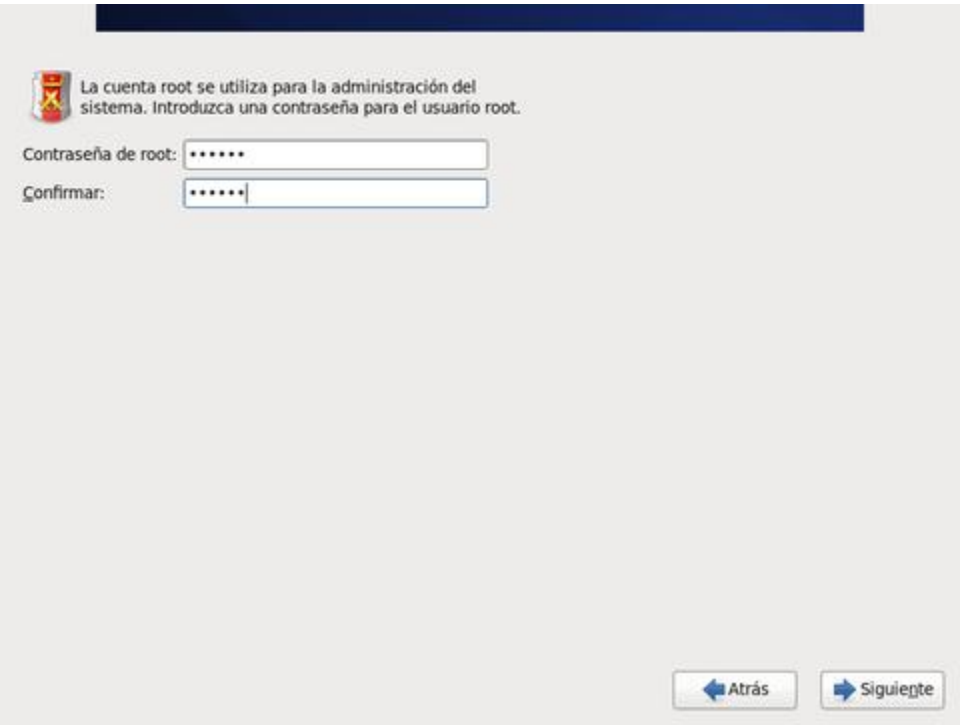
Seleccione la zona horaria que corresponda a su localidad, **haciendo clic** sobre cualquier punto en el mapamundi. Se recomienda dejar seleccionada la casilla **«El reloj del sistema utiliza UTC.»** Ésto último significa que el reloj del sistema utilizará **UTC** (**T**iempo **U**niversal **C**oordinado), que es el sucesor de **GMT** (b>Greenwich **M**ean **T**ime, que significa Tiempo Promedio de Greenwich) y es la zona horaria de referencia respecto a la cual se calculan todas las otras zonas horarias del mundo. Al terminar, haga clic sobre el botón denominado **«Siguiente.»**



Defina y confirme la contraseña para el usuario **root**, cuenta que será utilizada para la administración del sistema. Al terminar, haga clic sobre el botón denominado **«Siguiente.»**

Nota.

Evite utilizar palabras de diccionario y datos personales, procurando utilizar al menos 8 caracteres, en combinaciones de números, letras mayúsculas, letras minúsculas y otros caracteres.



La siguiente pantalla le dará a elegir las opciones para crear las particiones en el disco duro. Salvo que elija **«Crear un diseño personalizado,»** invariablemente se aplicará un **diseño predeterminado**, el cual consistirá en:

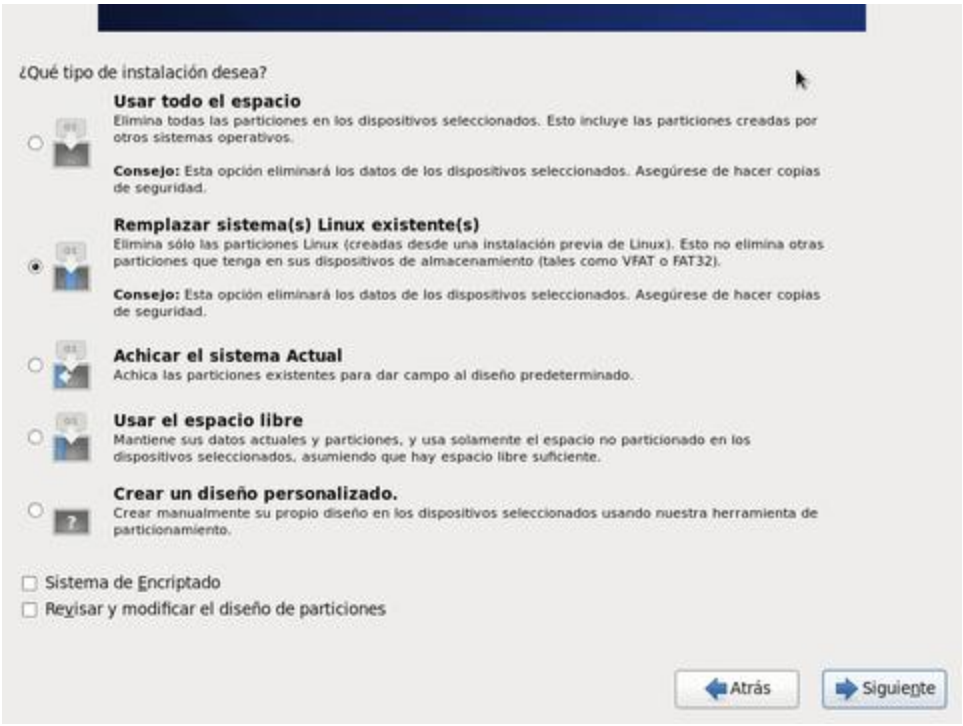
- Una partición estándar de 200 MB para **/boot**
- Un volumen lógico para **/**, que utilizará la mayor parte del espacio disponible y que posteriormente permitirá hacer crecer el sistema añadiendo otro disco duro, con unidades físicas que se añadirán al volumen lógico.
- Un volumen lógico para la **partición de memoria de intercambio** (*swap*), que en equipos con menos de 1 GM RAM, utilizará un espacio será equivalente al doble del RAM físico del sistema o bien, en equipos con más de 1 GB RAM, utilizará un espacio equivalente a la suma del RAM físico del sistema, más 2 GB.

Nota.

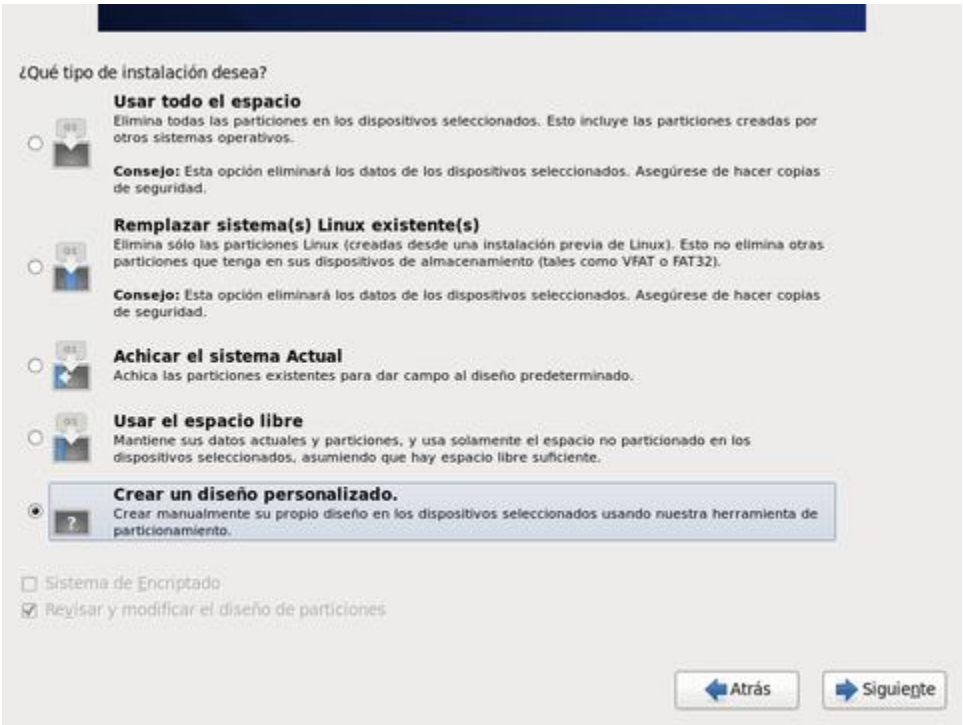
Este diseño predeterminado funcionará bien para cualquier servidor, con cualquier propósito, siempre que se trate de un equipo que permita añadir fácilmente más unidades de almacenamiento, para así aprovechar los volúmenes lógicos. Si se trata de una computadora portátil o sistema de escritorio, que carezca de alguna forma sencilla de añadir otro disco duro, este diseño predeterminado resultará totalmente inadecuado, pues se estará utilizando una función (volúmenes lógicos) que jamás se podrá aprovechar.

Las opciones en pantalla hacen lo siguiente:

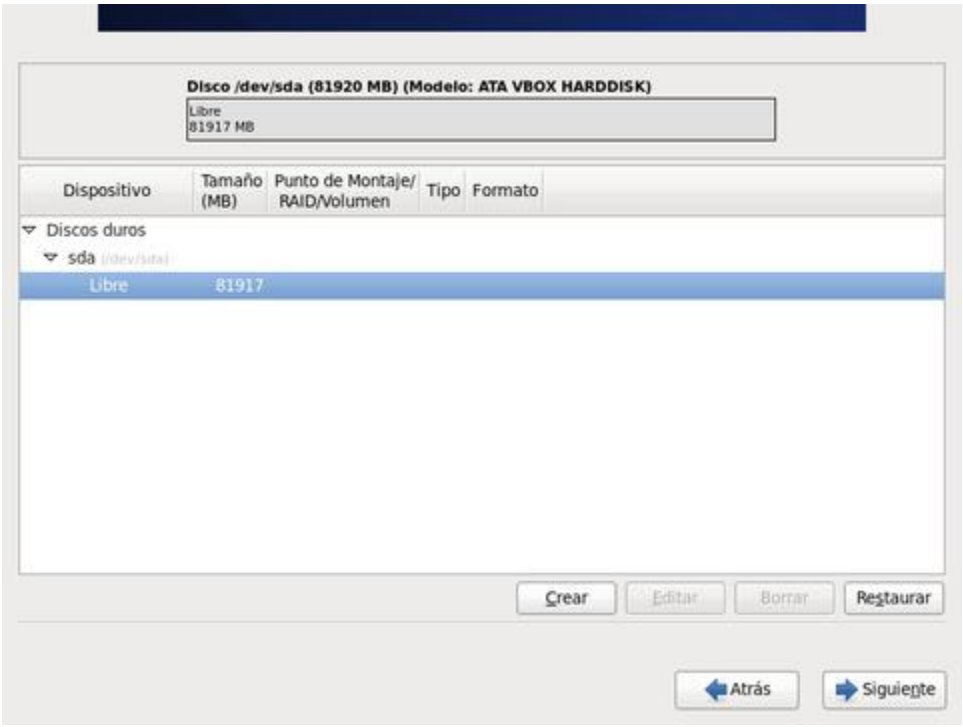
- **«Usar todo el espacio»**, eliminará cualquier partición de cualquier otro sistema operativo presente y creará de forma automática las particiones necesarias.
- **«Reemplazar sistema(s) Linux existente(s)»**, sólo eliminará todas las particiones Linux existentes y creará de forma automática las particiones necesarias.
- **«Achicar el sistema actual»**, cambiará el tamaño de las particiones existentes de otros sistemas operativos, como Windows, haciendo el espacio necesario para poder instalar un diseño predeterminado de particiones Linux.
- **«Usar espacio libre»**, creará de forma automática las particiones necesarias en el espacio disponible, basándose sobre un diseño predeterminado.
- **«Crear un diseño personalizado»**, permitirá elegir las particiones estándar o volúmenes lógicos, que uno requiera.



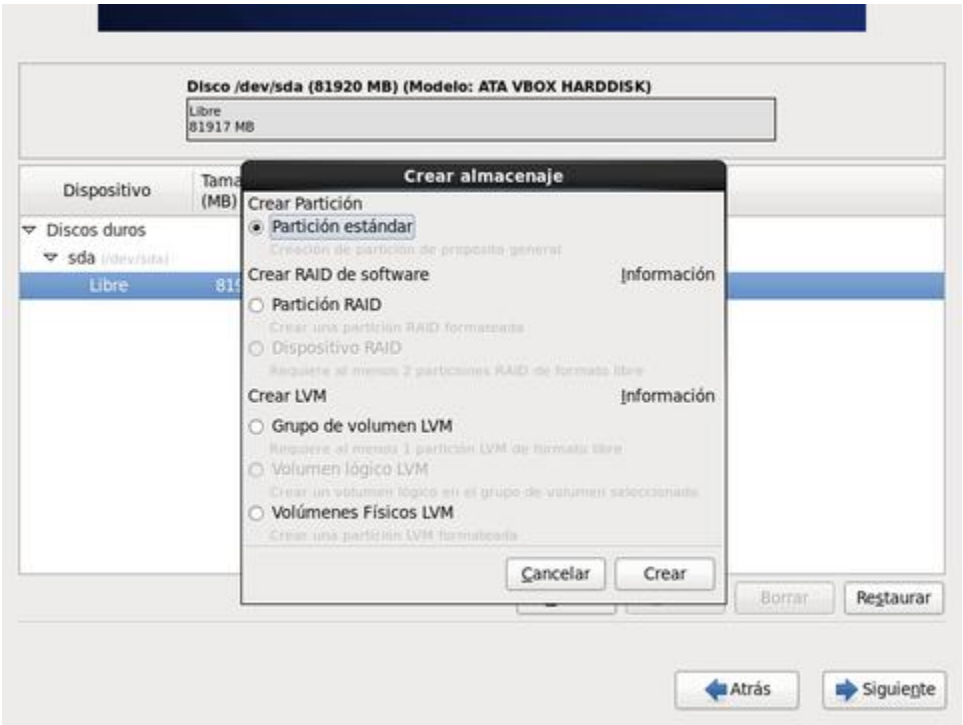
Seleccione **«Crear un diseño personalizado»** y haga clic sobre el botón denominado **«Siguiente.»**



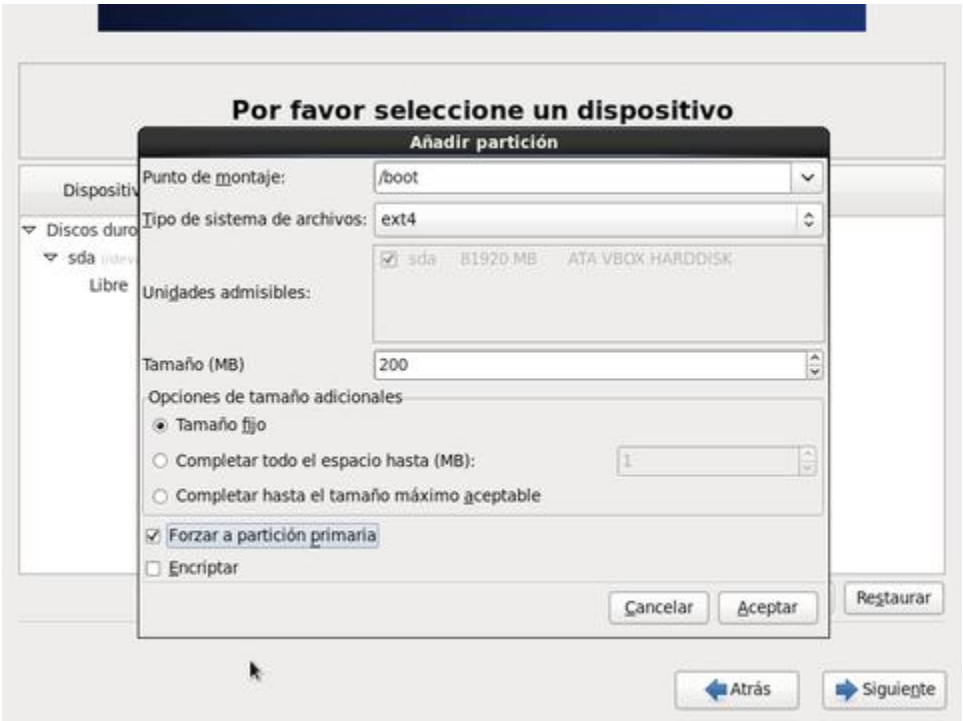
Se mostrará la tabla de particiones actual, mostrando el espacio libre disponible para crear nuevas particiones. Haga clic sobre el botón **«Crear.»**



Se abrirá una ventana donde podrá definir el tipo de partición a crear. Elija crear una **«Partición estándar.»** Al terminar, haga clic sobre el botón **«Crear.»**



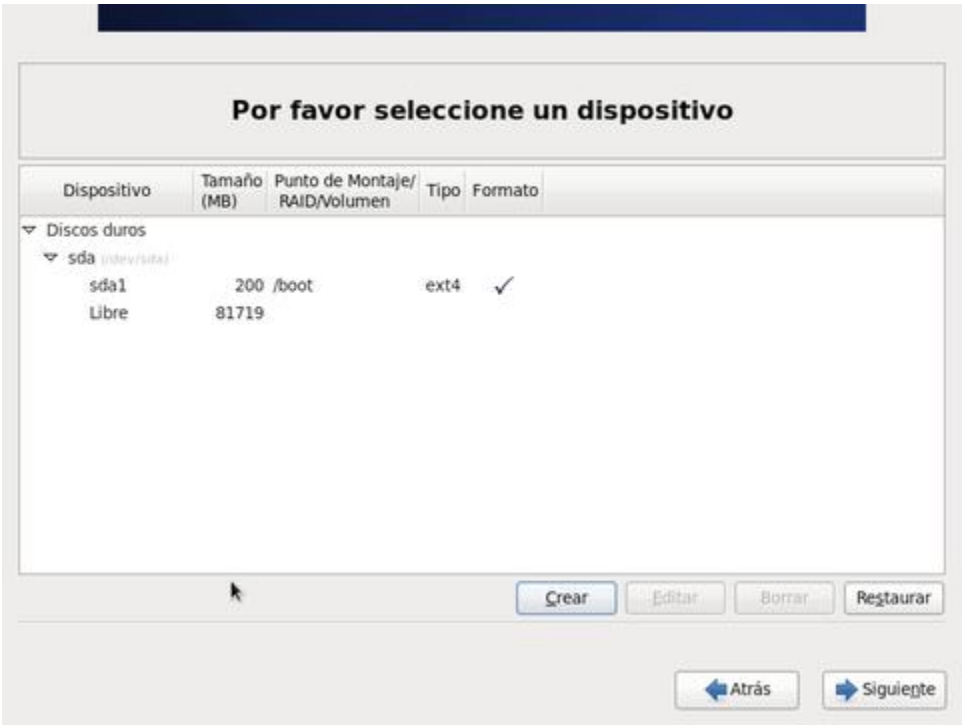
En la ventana que aparece sobre la tabla de particiones, defina **/boot** como punto de montaje, mantenga el formato ext4, mantenga el tamaño de 200 MB y active la casilla de opción denominada **«Forzar a partición primaria.»** Al terminar, haga clic sobre el botón **«Aceptar.»**



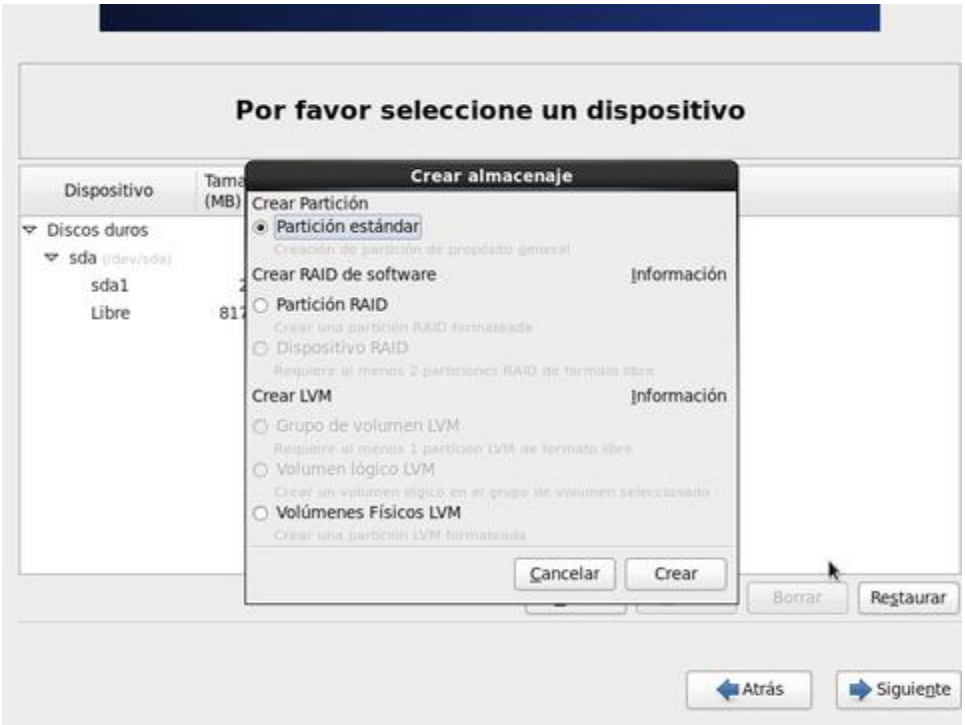
Nota.

Ext4 (fourth extended filesystem o cuarto sistema de archivos extendido) es, al igual que ext3, un sistema de archivos con registro por diario, con muchas mejoras respecto de ext3, entre las que se incluyen, entre otras cosas, el soporte de volúmenes de hasta 1024 PiB, soporte añadido de extents (conjunto de bloques físicos contiguos), menor uso de recursos de sistema, mejoras sustanciales en la velocidad de lectura y escritura y verificación más rápida con el mandato **fsck**. En resumen, prefiera utilizar ext4.

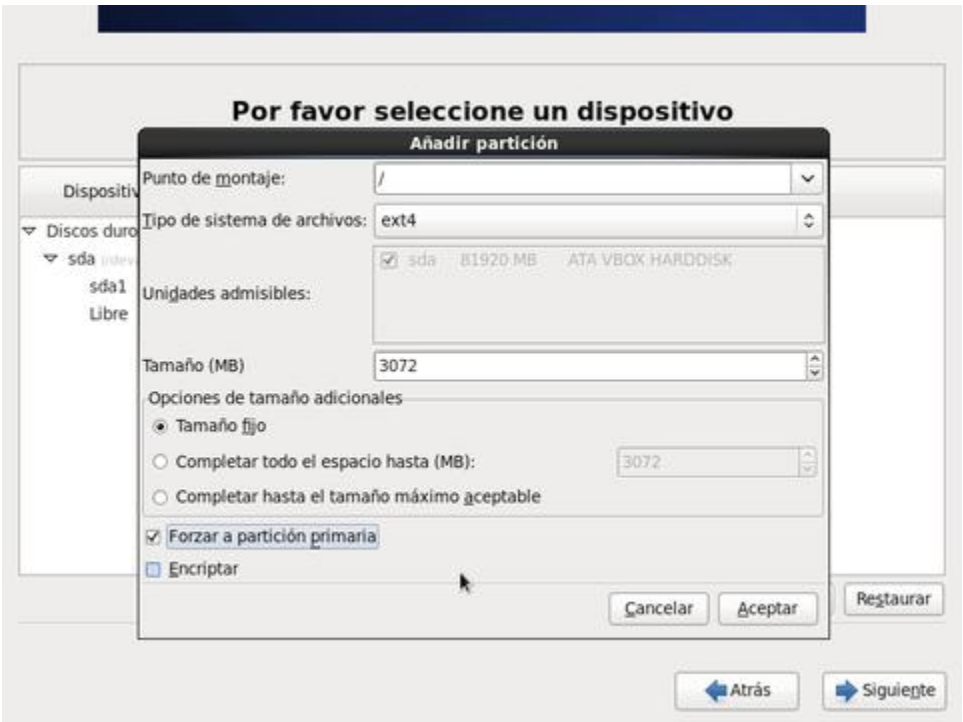
Se deberá mostrar la tabla de particiones, donde deberá aparecer la partición recién creada. Para añadir la siguiente partición, vuelva a hacer clic sobre el botón **«Crear.»**



Se abrirá una ventana donde podrá definir el tipo de partición a crear. Elija crear una **«Partición estándar.»** Al terminar, haga clic sobre el botón **«Crear.»**



En la ventana que aparece sobre la tabla de particiones, defina **/** como punto de montaje, mantenga el formato ext4 y defina un tamaño de **3072 MB** y active la casilla de opción denominada **«Forzar a partición primaria.»** Al terminar, haga clic sobre el botón **«Aceptar.»**



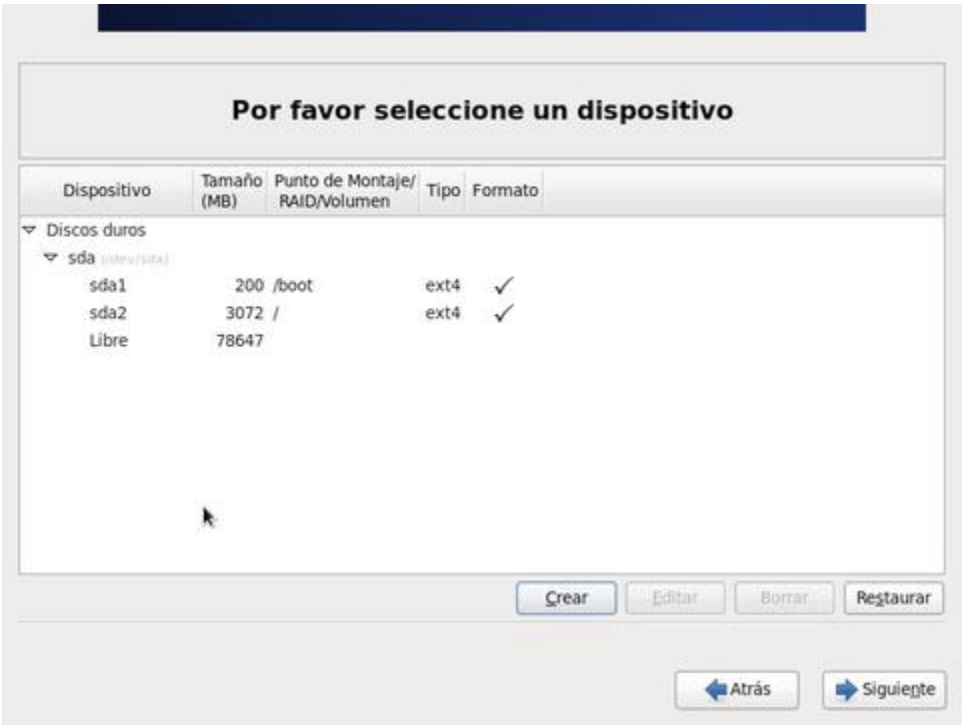
Nota.

Sólo se recomienda definir como **particiones primarias** a las correspondientes a **/boot** y **/**, con la finalidad de que éstas sean creadas entre los primeros sectores del disco duro o unidad de almacenamiento y para evitare que incidentalmente queden incluidas dentro de la **partición extendida**. Esta última se creará de manera automática después como la cuarta partición del disco duro, dentro de la cual se crearán cuantas **particiones lógicas** como sean necesarias.

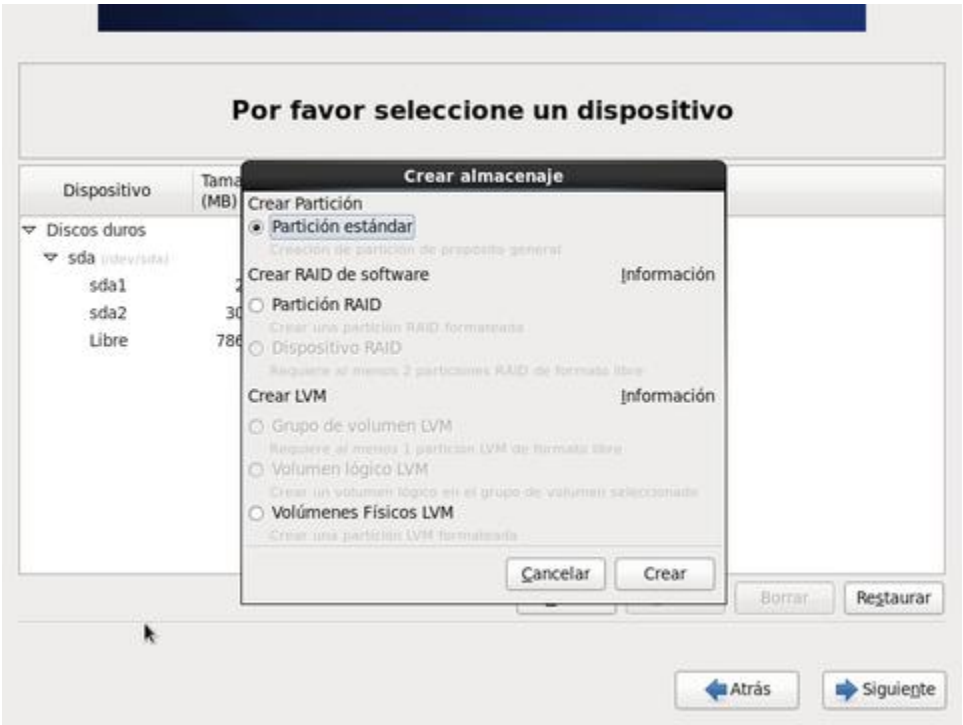
Nota.

Los sistemas modernos, basados sobre arquitectura Intel, tienen un límite máximo de cuatro particiones. Se puede utilizar un diseño de **hasta cuatro particiones primarias** o bien un diseño de **tres particiones primarias** y **una partición extendida** (sólo puede haber una por unidad de almacenamiento), dentro de la cual se pueden crear hasta once **particiones lógicas**, las cuales en realidad son sub-particiones de la **partición extendida**. GNU/Linux permite utilizar hasta un máximo de 15 particiones (total de particiones primarias, más la partición extendida, más las particiones lógicas).

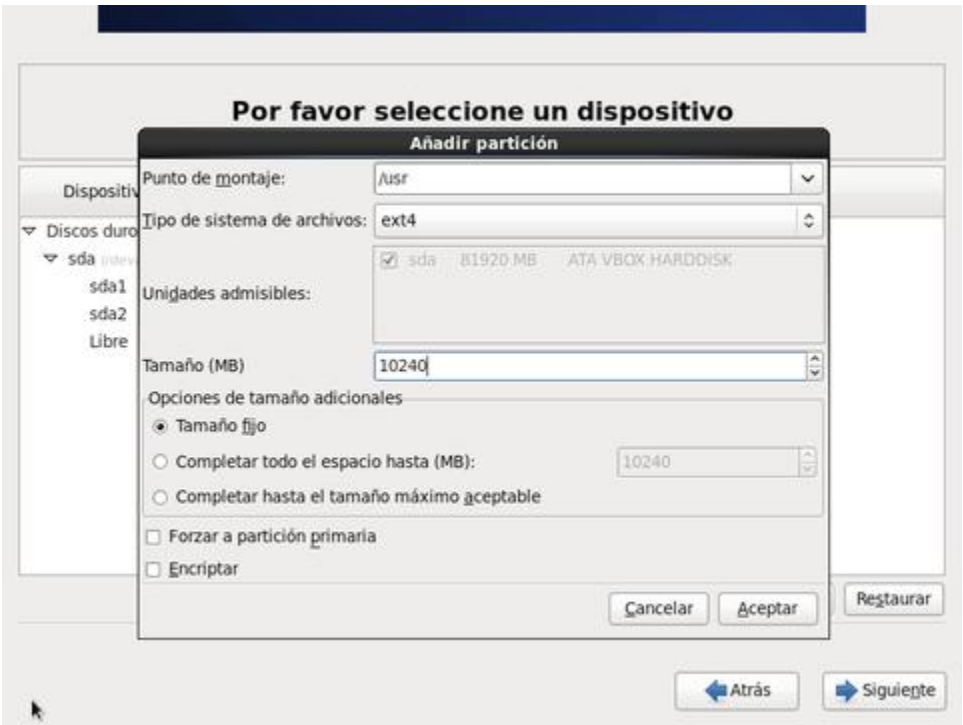
Se deberá mostrar la tabla de particiones, donde deberá aparecer la partición recién creada. Para añadir la siguiente partición, vuelva a hacer clic sobre el botón **«Crear.»**



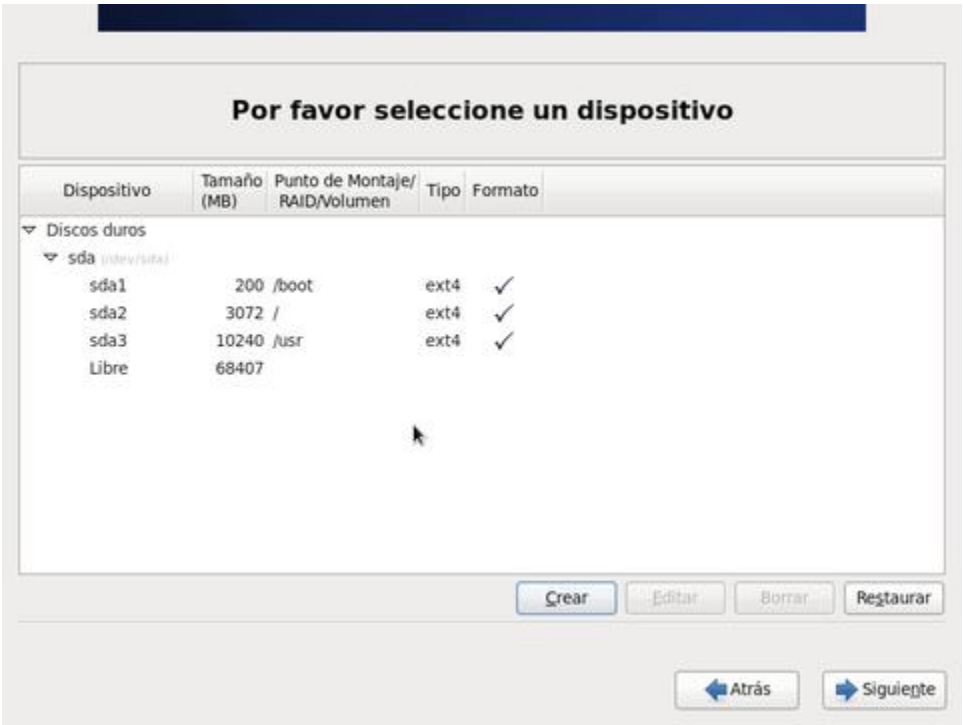
Se abrirá una ventana donde podrá definir el tipo de partición a crear. Elija crear una **«Partición estándar.»** Al terminar, haga clic sobre el botón **«Crear.»**



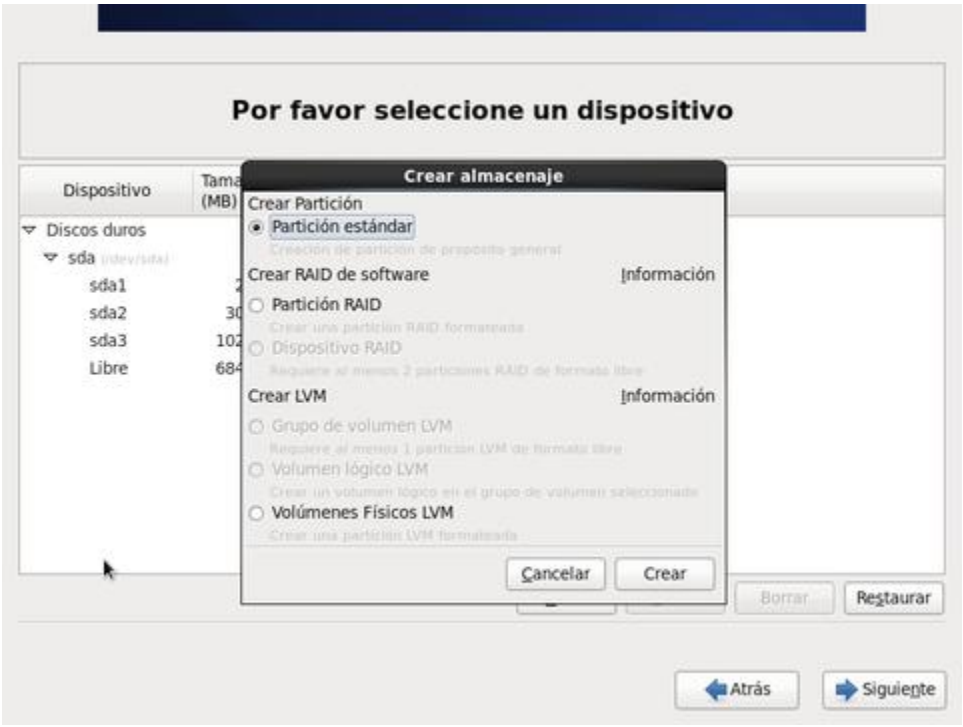
En la ventana que aparece sobre la tabla de particiones, defina **/usr** como punto de montaje, mantenga el formato ext4 y defina un tamaño de **10240 MB** o más, si considera que ocupará más espacio para alguna aplicación o conjunto de aplicaciones, en particular. Al terminar, haga clic sobre el botón **«Aceptar.»**



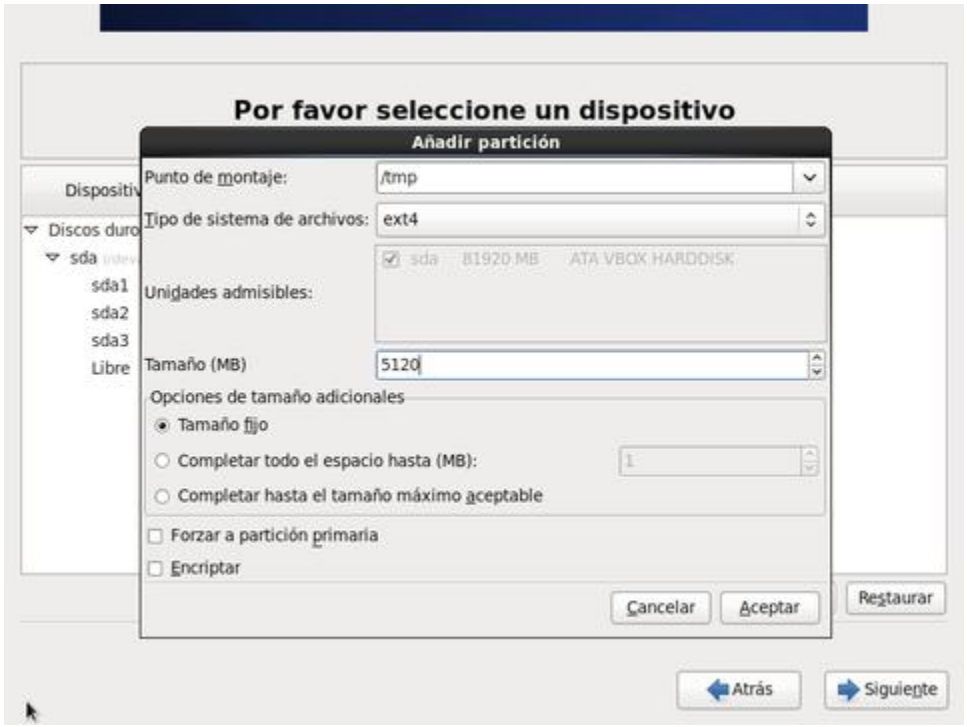
Se deberá mostrar la tabla de particiones, donde deberá aparecer la partición recién creada. Para añadir la siguiente partición, vuelva a hacer clic sobre el botón **«Crear.»**



Se abrirá una ventana donde podrá definir el tipo de partición a crear. Elija crear una **«Partición estándar.»** Al terminar, haga clic sobre el botón **«Crear.»**



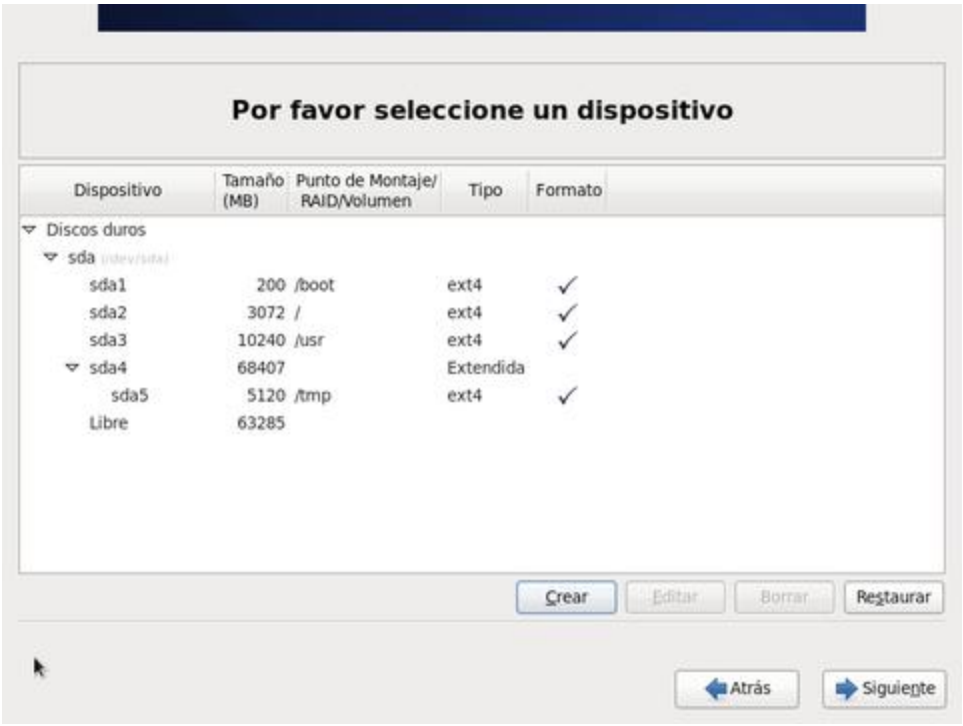
En la ventana que aparece sobre la tabla de particiones, defina **/tmp** como punto de montaje, mantenga el formato ext4 y defina un tamaño de **5120 MB**. Al terminar, haga clic sobre el botón **«Aceptar.»**


Por favor seleccione un dispositivo
Añadir partición
Punto de montaje:
/tmp
Tipo de sistema de archivos:
ext4
Unidades admisibles:
sda 81920 MB ATA VBOX HARDDISK
Tamaño (MB)
5120
Opciones de tamaño adicionales
Tamaño fijo
Completar todo el espacio hasta (MB):
Completar hasta el tamaño máximo aceptable
Forzar a partición primaria
Encriptar
Cancelar
Aceptar
Dispositiv
Discos duro
sda
sda1
sda2
sda3
Libre
Restaurar
Atrás
Siguiente

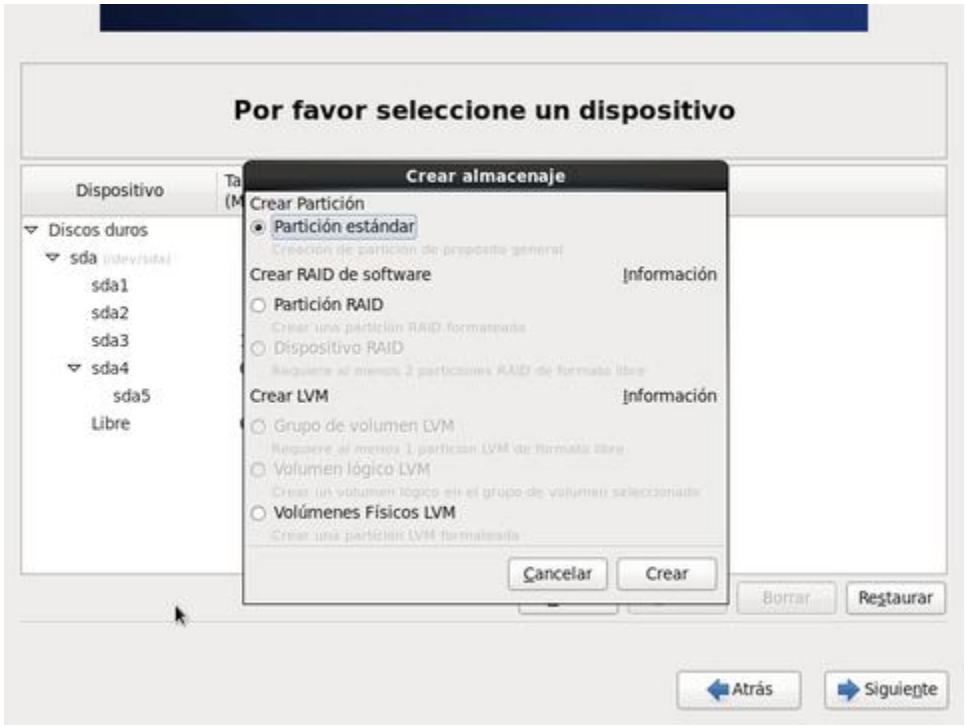
Nota.

El tamaño de la partición para **/tmp** dependerá del tipo de aplicaciones que se utilizarán posterior a la instalación. Consulte la documentación del programa o aplicación que tenga planeado utilizar. Para la mayoría de los casos, será más que suficiente con asignar **5120 MB**.

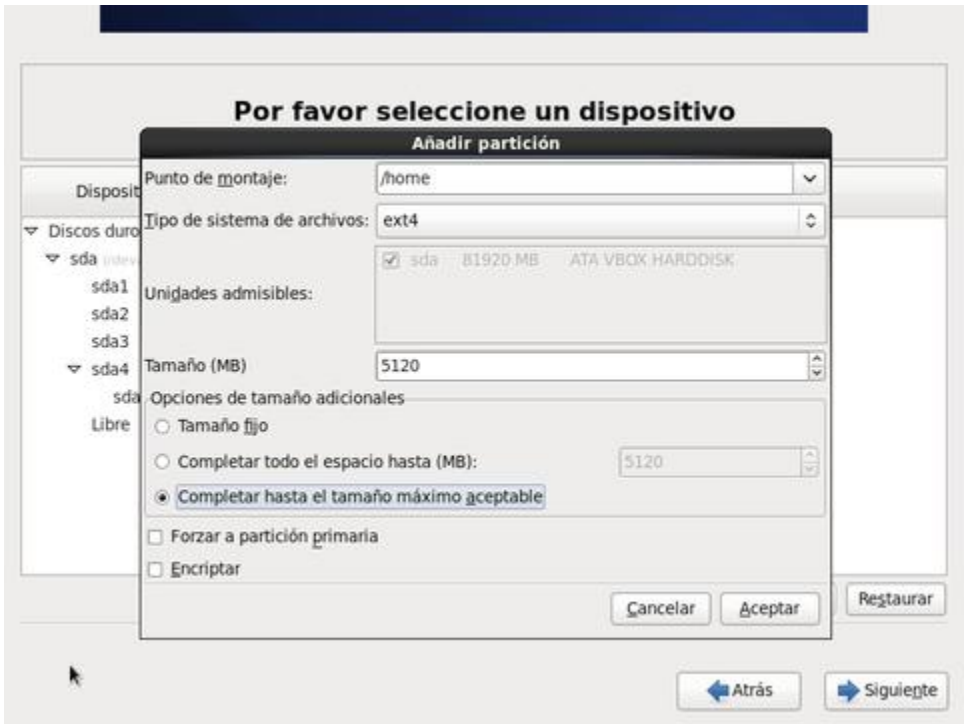
Se deberá mostrar la tabla de particiones, donde deberá aparecer la partición recién creada. Para añadir la siguiente partición, vuelva a hacer clic sobre el botón **«Crear.»**



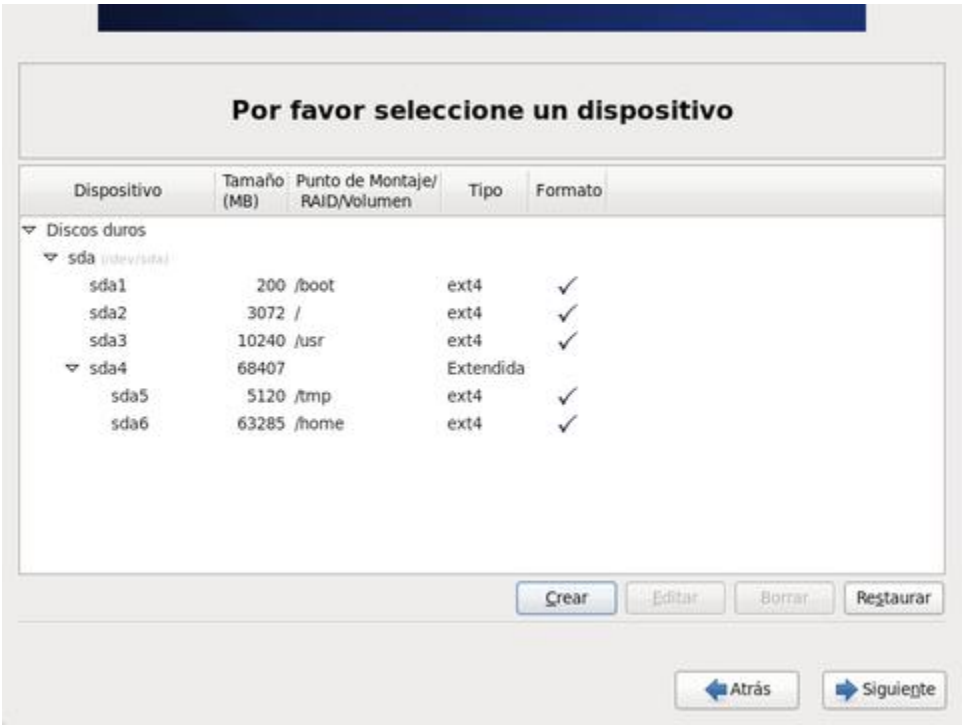
Se abrirá una ventana donde podrá definir el tipo de partición a crear. Elija crear una **«Partición estándar.»** Al terminar, haga clic sobre el botón **«Crear.»**



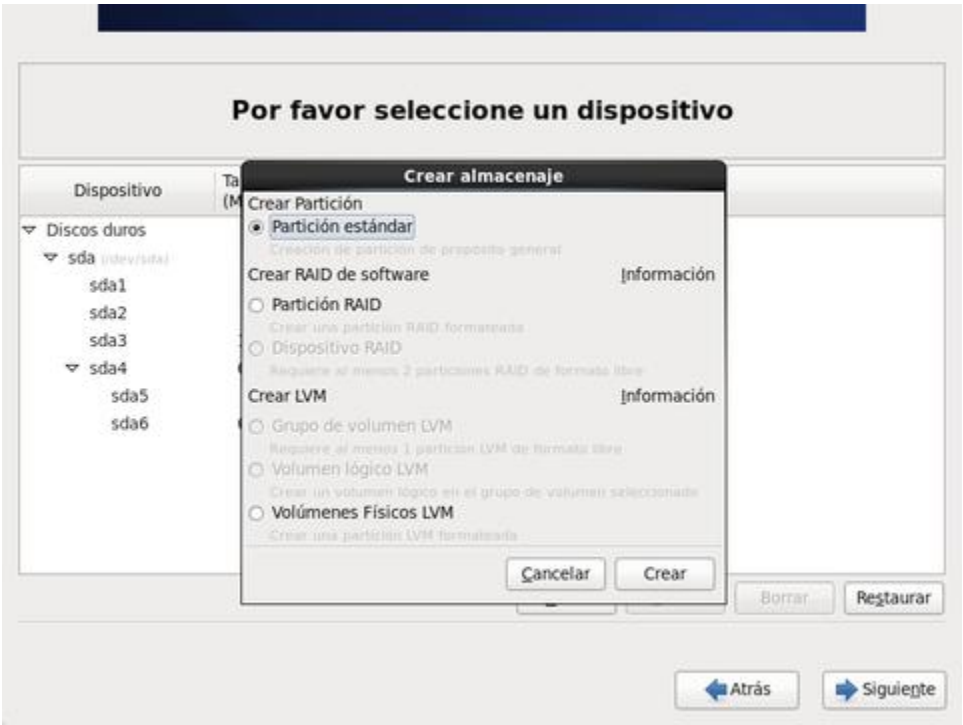
En la ventana que aparece sobre la tabla de particiones, defina **/home** como punto de montaje, mantenga el formato ext4 y elija la casilla de opción denominada **«Completar hasta el tamaño máximo aceptable.»** Al terminar, haga clic sobre el botón **«Aceptar.»**



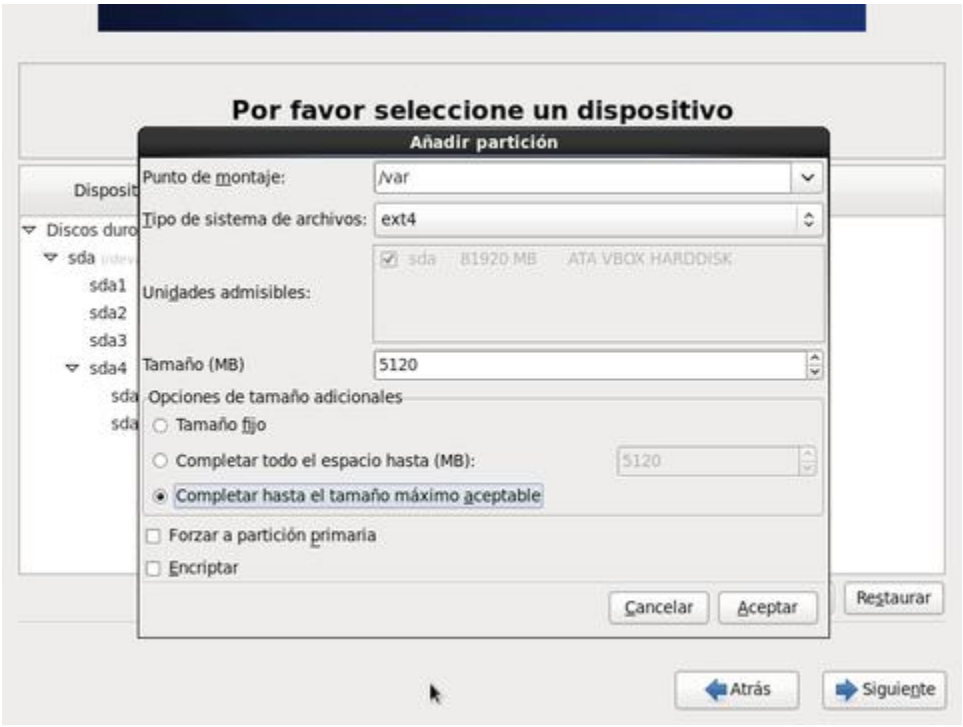
Se deberá mostrar la tabla de particiones, donde deberá aparecer la partición recién creada. **Temporalmente** notará que **/home** tiene asignado todo el espacio de almacenamiento que anteriormente estaba libre. En cuanto haya creado la partición **/var**, ambas se repartirán nuevamente el espacio, casi equitativamente. Para añadir la siguiente partición, vuelva a hacer clic sobre el botón **«Crear.»**



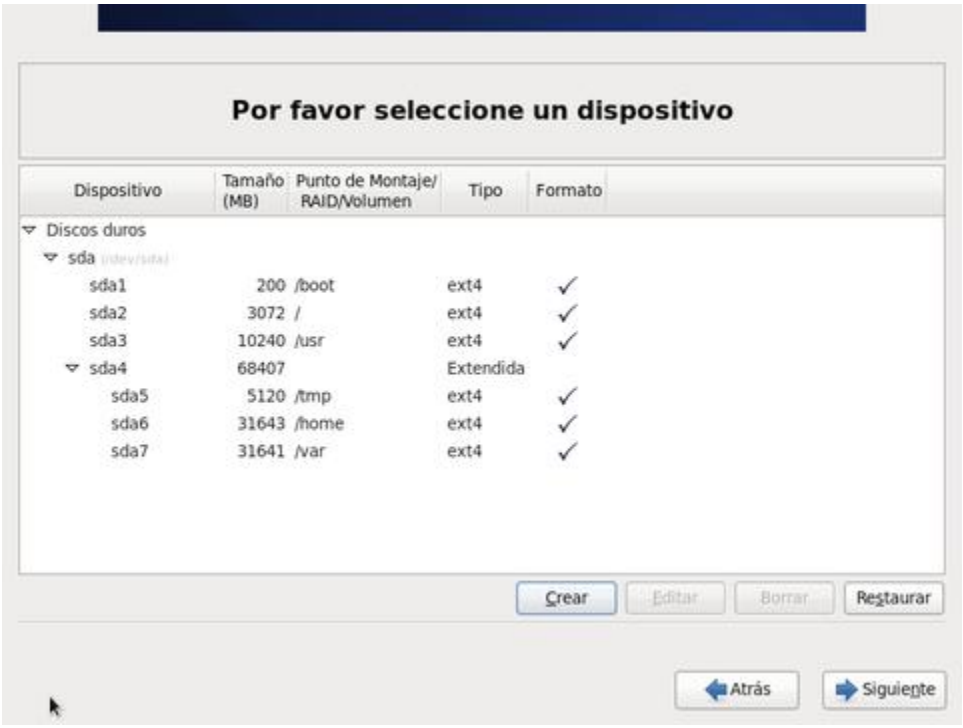
Se abrirá una ventana donde podrá definir el tipo de partición a crear. Elija crear una **«Partición estándar.»** Al terminar, haga clic sobre el botón **«Crear.»**



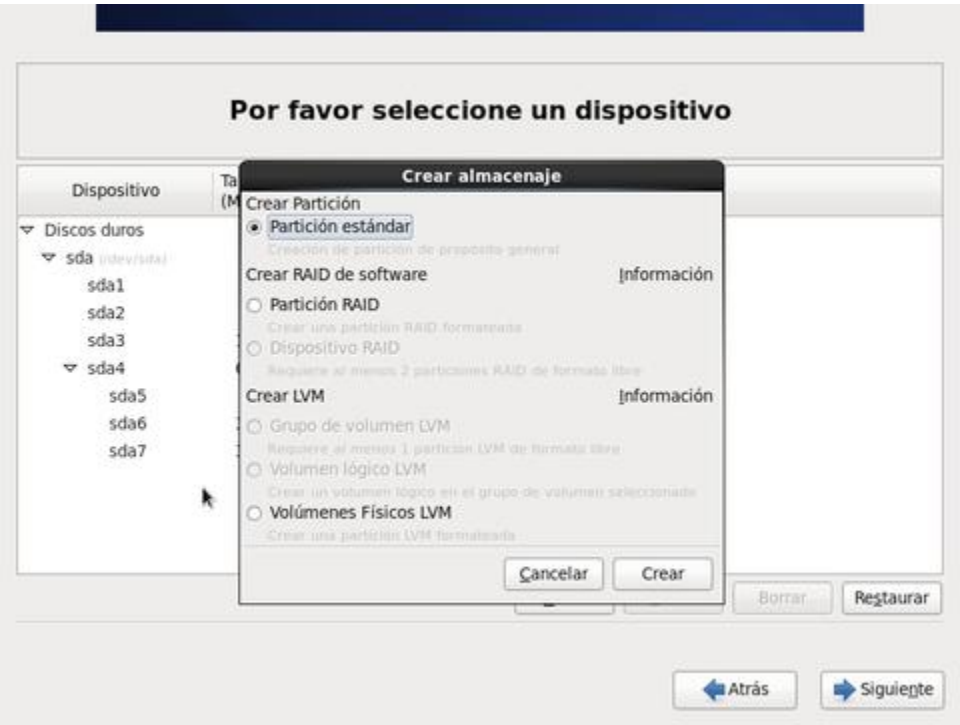
En la ventana que aparece sobre la tabla de particiones, defina **/var** como punto de montaje, mantenga el formato ext4 y elija la casilla de opción denominada **«Completar hasta el tamaño máximo aceptable.»** Al terminar, haga clic sobre el botón **«Aceptar.»**



Se deberá mostrar la tabla de particiones, donde deberá aparecer la partición recién creada. **Temporalmente** notará que **/home** y **/var** se han repartido el espacio disponible. Para añadir la última partición, la correspondiente a la de la memoria de intercambio, vuelva a hacer clic sobre el botón **«Crear.»**

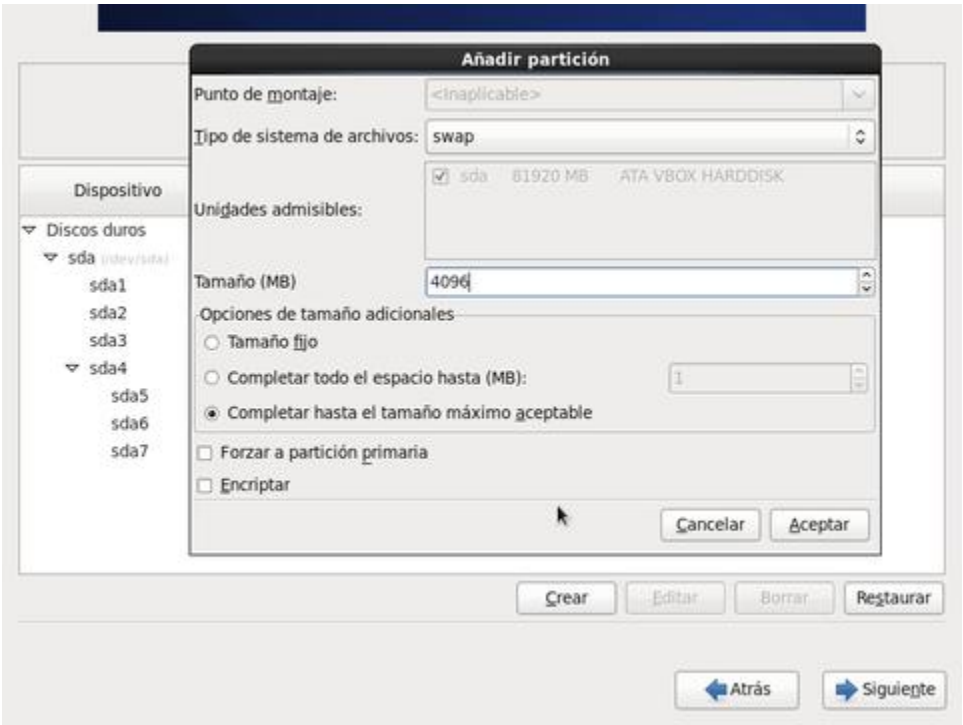


Se abrirá una ventana donde podrá definir el tipo de partición a crear. Elija crear una **«Partición estándar.»** Al terminar, haga clic sobre el botón **«Crear.»**

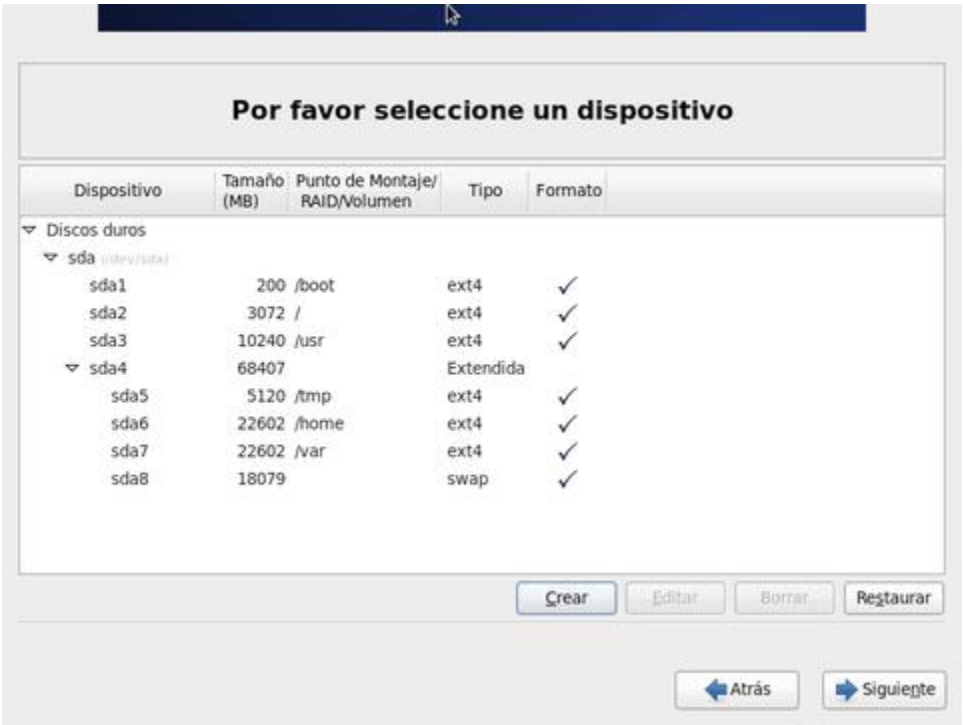


Para el tamaño de la partición de memoria de intercambio (*swap*), siga las siguientes reglas:

- **Si el sistema tiene menos de 1 GB RAM:** Defina una cantidad equivalente a dos veces la cantidad de RAM físico. Ejemplos:
  - Si el sistema tiene 512 MB RAM, defina 1024 MB para la partición de memoria de intercambio.
  - Si el sistema tiene 768 MB RAM, defina 1536 de memoria de intercambio.
  - Si el sistema tiene 1 GB RAM, defina 2048 MB para la partición de memoria de intercambio.
- **Si el sistema tiene más de 1 GB RAM:** Defina una cantidad equivalente a la suma de la cantidad de RAM físico, más 2 GB. Ejemplos:
  - Si el sistema tiene 1.5 GB RAM, defina 3584 MB para la partición de memoria de intercambio.
  - Si el sistema tiene 2 GB RAM, defina 4096 MB para la partición de memoria de intercambio.
  - Si el sistema tiene 4 GB RAM, defina 6144 MB para la partición de memoria de intercambio.
  - Si el sistema tiene 8 GB RAM, defina 10240 MB para la partición de memoria de intercambio.



Se mostrará la tabla de particiones. Note que la partición de intercambio ha tomado la mitad de su espacio asignado a costa de **/home** y la otra mitad a costa de **/var**. Examine a detalle y verifique que estén presentes todas las particiones que se planearon, asegurándose que tengan los tamaños aproximados a lo que se especificó en los pasos anteriores. Si está conforme con el diseño, haga clic sobre el botón denominado **«Siguiente.»**



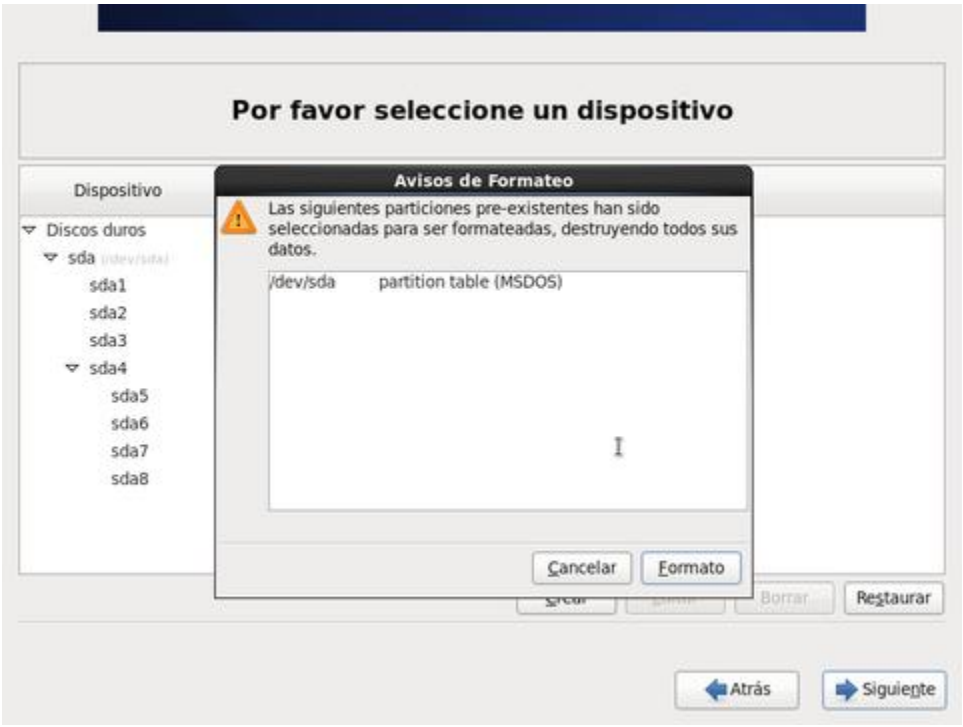
Nota.

Otras particiones recomendadas pueden ser **/var/lib** y **/var/www**. Asignar como particiones a estos directorios permitirá posteriormente optimizarlas, sólo cambiando el formato del registro por diario (*journal*). Para más detalles consulte el documento titulado «**Como optimizar el sistema de archivos ext3 y ext4**,» con la finalidad de conocer los procedimientos necesarios para optimizar el sistema de archivos después de terminar la instalación, luego de que inicie el sistema operativo por primera vez. Puede asignar a cada una de estas particiones cuanto espacio como considere necesario para necesidades particulares.

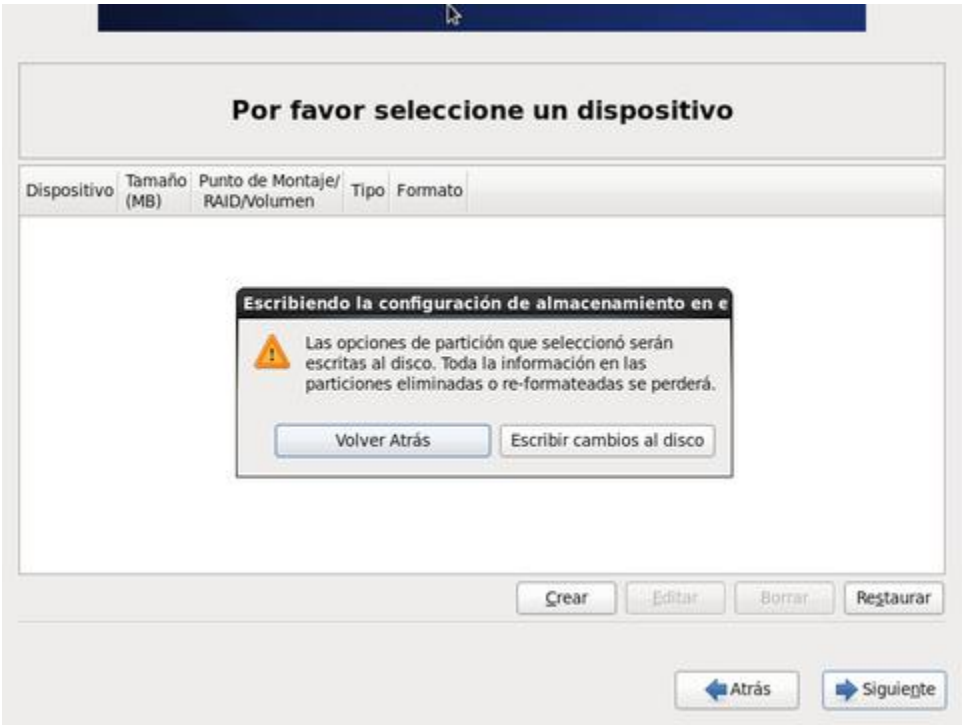
Siendo que **/var/lib** suele utilizarse principalmente para almacenar bases de datos, servidores directorios, como LDAP y otros tipos de datos, sobre los cuales se realiza lectura y escritura simultánea, conviene optimizar el registro por diario de esta partición, utilizando el formato **journal**, obteniendo como resultado un mejor rendimiento para las bases de datos y servidores de directorios, como LDAP.

Si **/var/www** va a contener los archivos de un portal de Internet y éstos sufrirán pocos cambios o bien sufrirán cambios poco frecuentes, conviene optimizar el registro por diario de esta partición, utilizando el formato **writeback**, obteniendo como resultado una mejor velocidad de lectura.

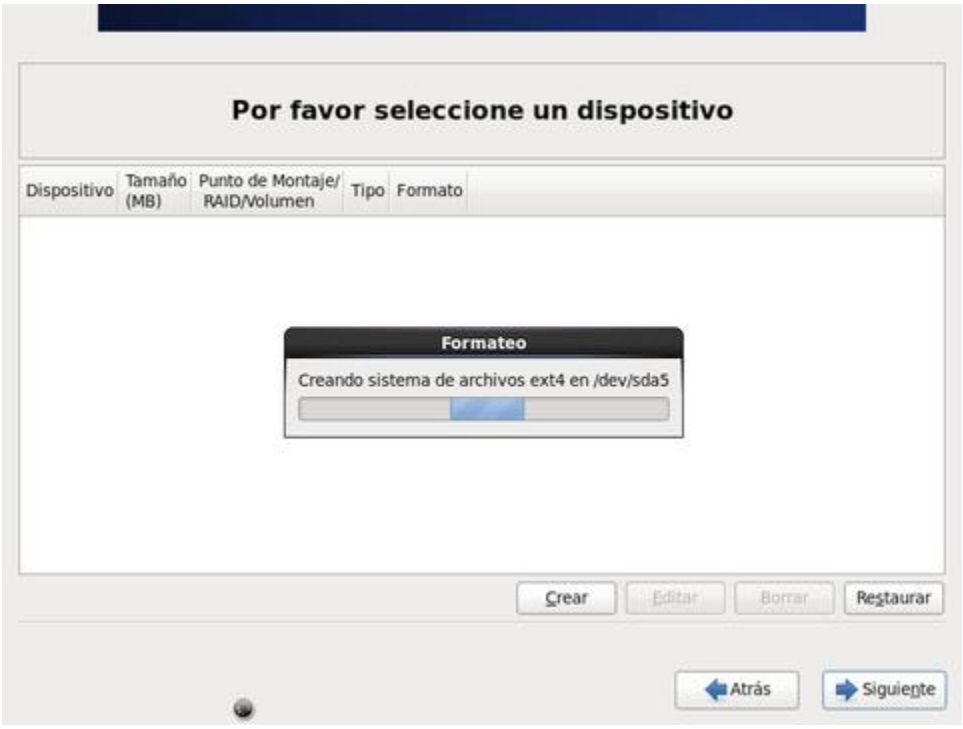
Se solicitará que confirme de manera explícita que se procederá a eliminar o dar formato a particiones existentes en el medio de almacenamiento. Si desea proceder, haga clic sobre el botón **«Formato.»**



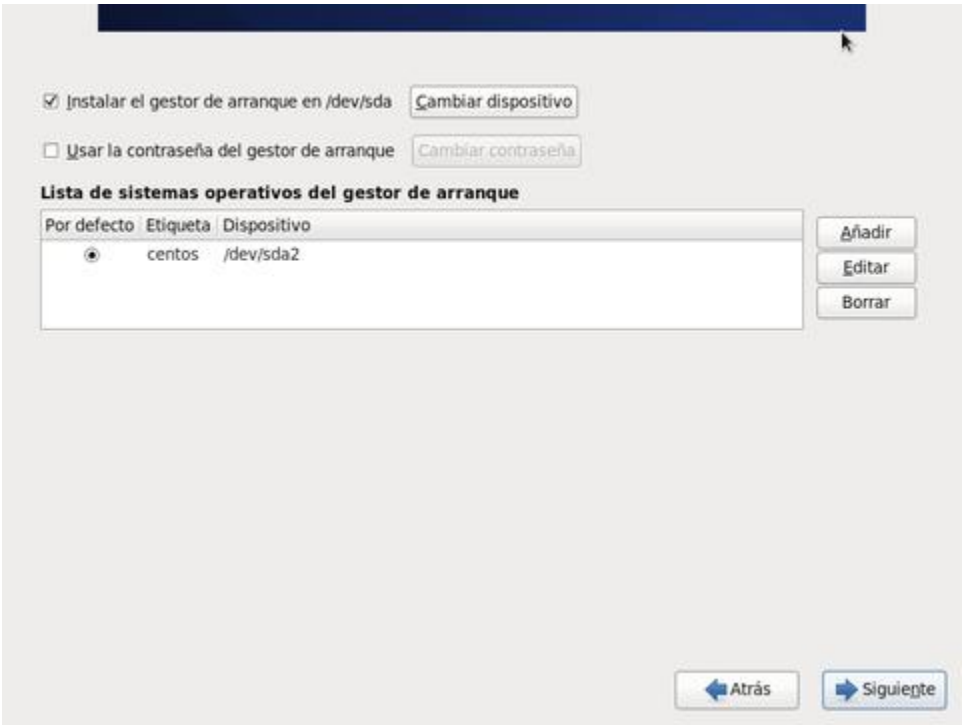
Se solicitará confirme que desea escribir los cambios al disco duro. Si desea proceder, haga clic sobre el botón **«Escribir cambios al disco.»**



Espere algunos minutos mientras de guarda la tabla de particiones y se da formato a todas las particiones definidas en los pasos anteriores.

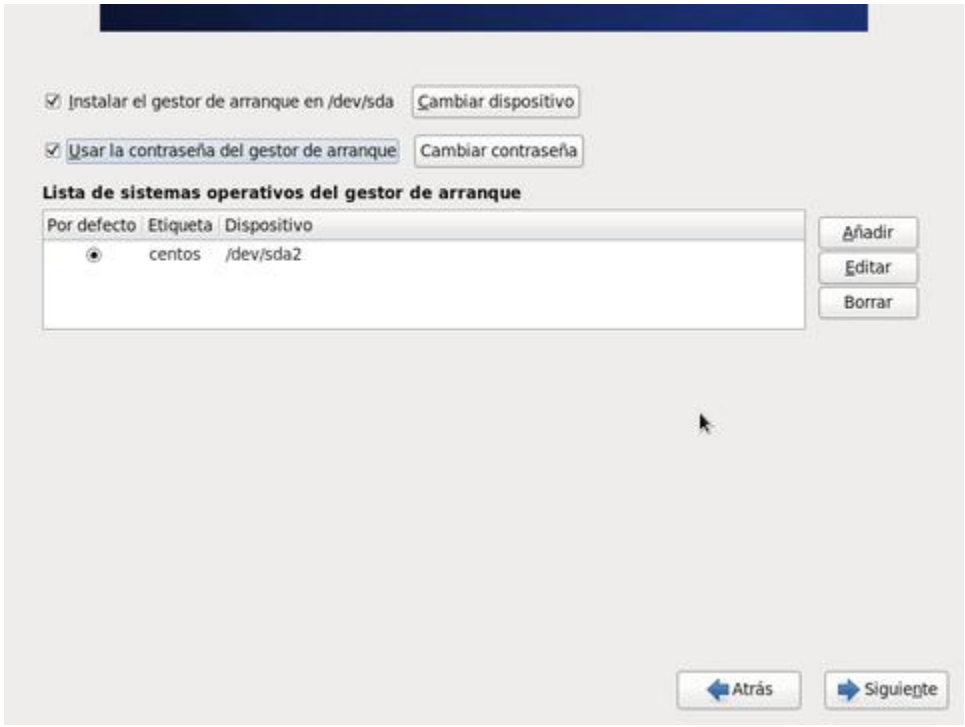


Por seguridad, conviene asignar una contraseña al gestor de arranque. Ésto tiene como finalidad el de evitar que cualquiera que tenga acceso físico al sistema, pueda modificar los parámetros de arranque del gestor de arranque e iniciar en modo mono-usuario (nivel de ejecución 1). Si desea proceder, haga clic sobre la casilla de opción denominada **«Usar la contraseña del gestor de arranque.»**

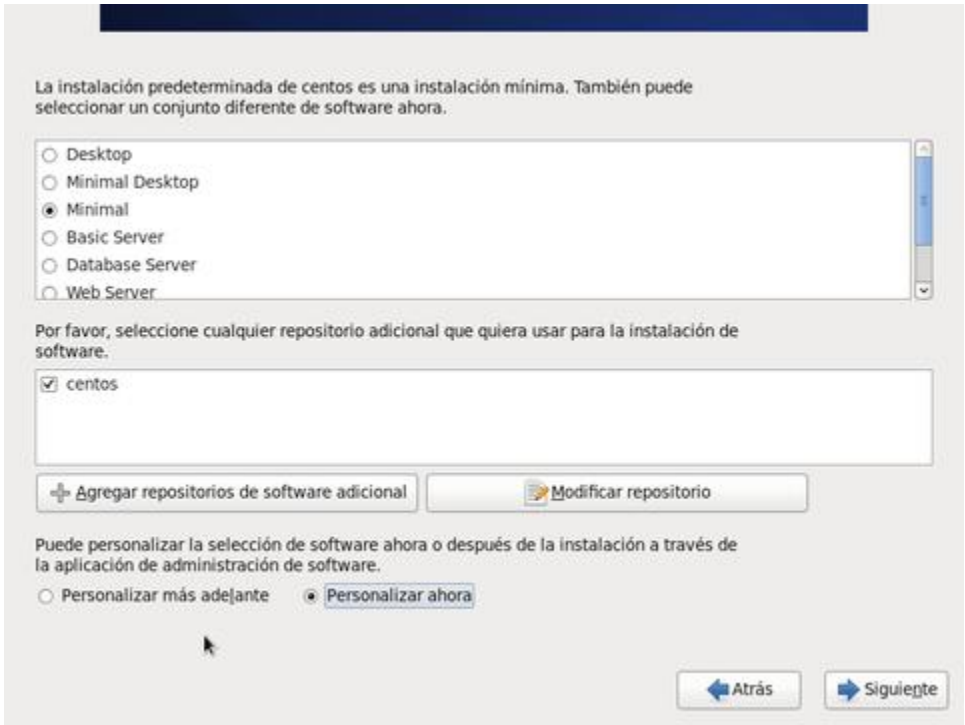


Asigne y confirme una contraseña para el gestor de arranque.

Al terminar, haga clic en el botón **«Siguiente.»**



Elija el tipo de instalación.



Nota.

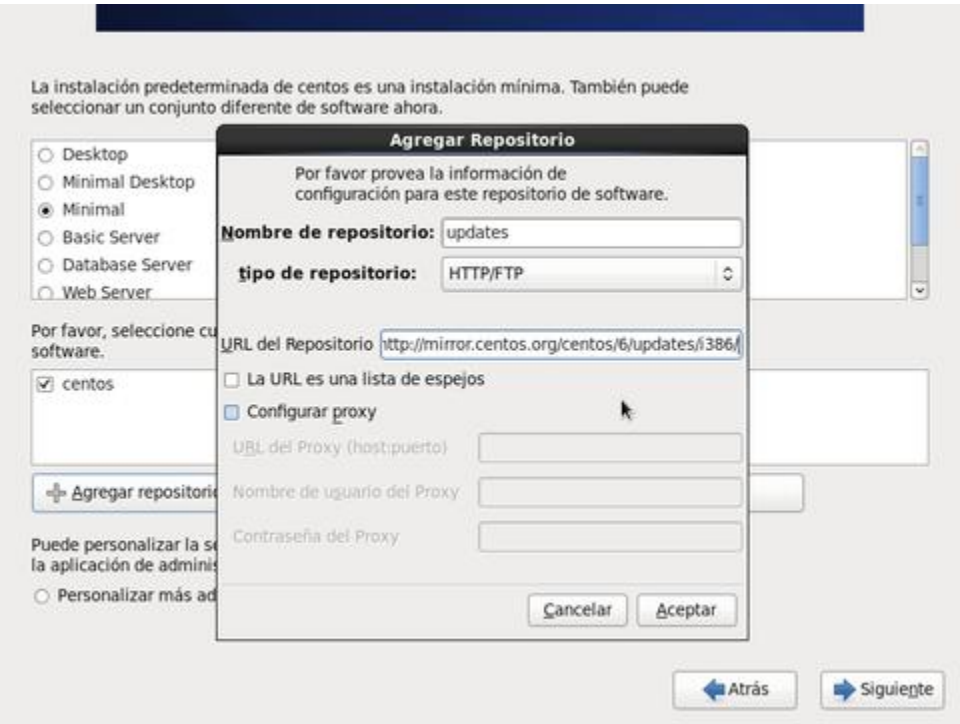
Es una buena práctica de seguridad el realizar una **instalación mínima** (casilla de opción **«Minimal»**) y posteriormente ir instalando sólo los paquetes que realmente se requieran. Mientras menos paquetes estén instalados, habrá menos servicios por los cuales preocuparse, además de que serán menores las descargas de paquetes durante las actualizaciones que realice periódicamente. La **instalación mínima** consiste del núcleo del sistema, un conjunto de mandatos básicos, lo necesario para configurar las interfaces de red, herramientas básicas para administrar el sistema de archivos, un conjunto básico de políticas para SELinux, el mandato yum y lo mínimo necesario para tener un sistema operativo funcional en modo texto.

Nota.

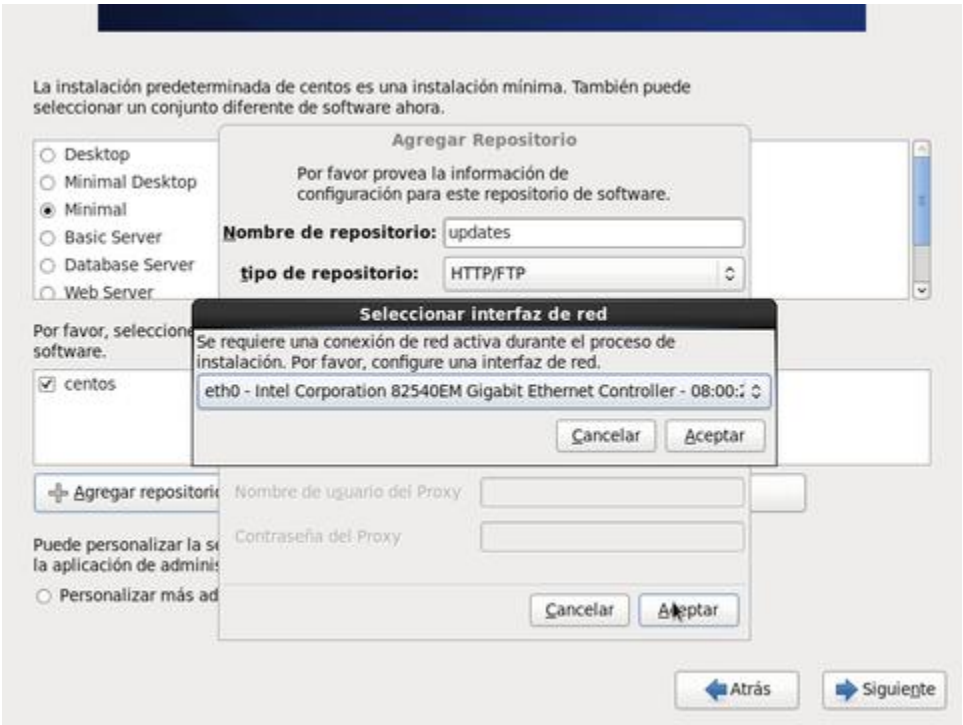
Tras finalizar la instalación y una vez que inicie por primera vez el sistema operativo, se recomienda instalar, a través del mandato **yum**, los paquetes **system-config-firewall-tui**, **system-config-network-tui**, **policycoreutils-python**, **selinux-policy-targeted**, **selinux-policy-mls**, **vim-enhanced**, **wget**, **bind-utils** y **openssh-clients**.

```
yum -y install system-config-firewall-tui openssh-clients
yum -y install system-config-network-tui bind-utils
yum -y install policycoreutils-python
yum -y install selinux-policy-targeted selinux-policy-mls
yum -y install vim-enhanced wget
```

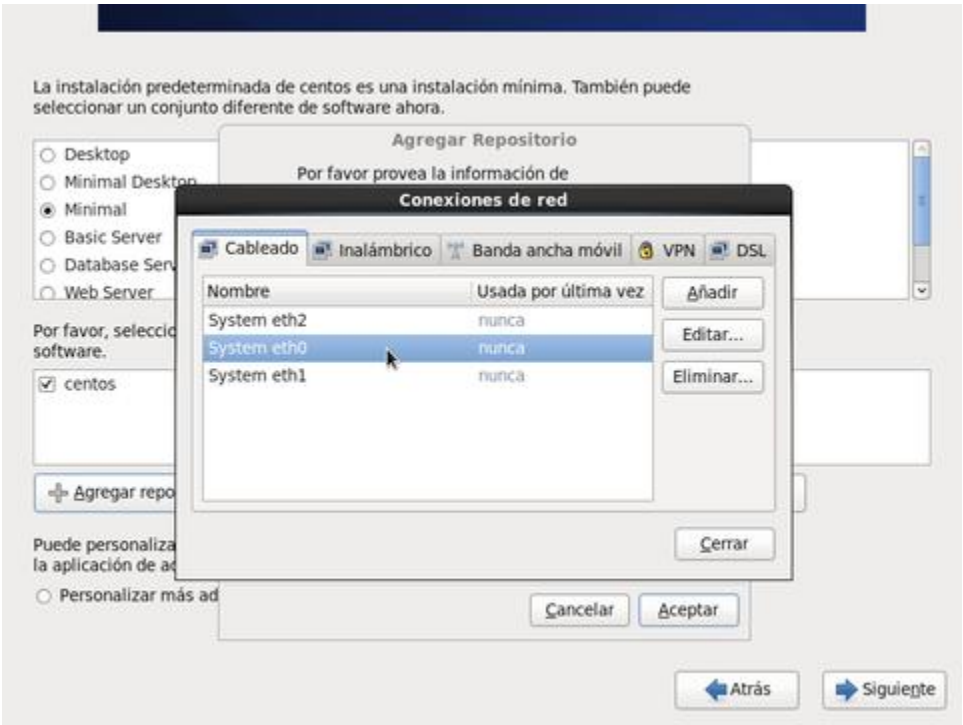
Si desea aplicar de una vez las actualizaciones y parches de seguridad disponibles, lo cual sería una excelente práctica de seguridad, haga clic sobre el botón denominado **«+ Agregar repositorios de software adicional.»** Ésto abrirá una ventana donde podrá ingresar la dirección de cualquier sitio de Internet que haga espejo de las actualizaciones de CentOS 6. Si desconoce que dirección definir, utilice http://mirror.centos.org/centos/6/updates/i386/, si está instalando la edición i386 o bien http://mirror.centos.org/centos/6/updates/x86_64/, si está instalando la edición x86-64. Al terminar, haga clic sobre el botón **«Aceptar.»**



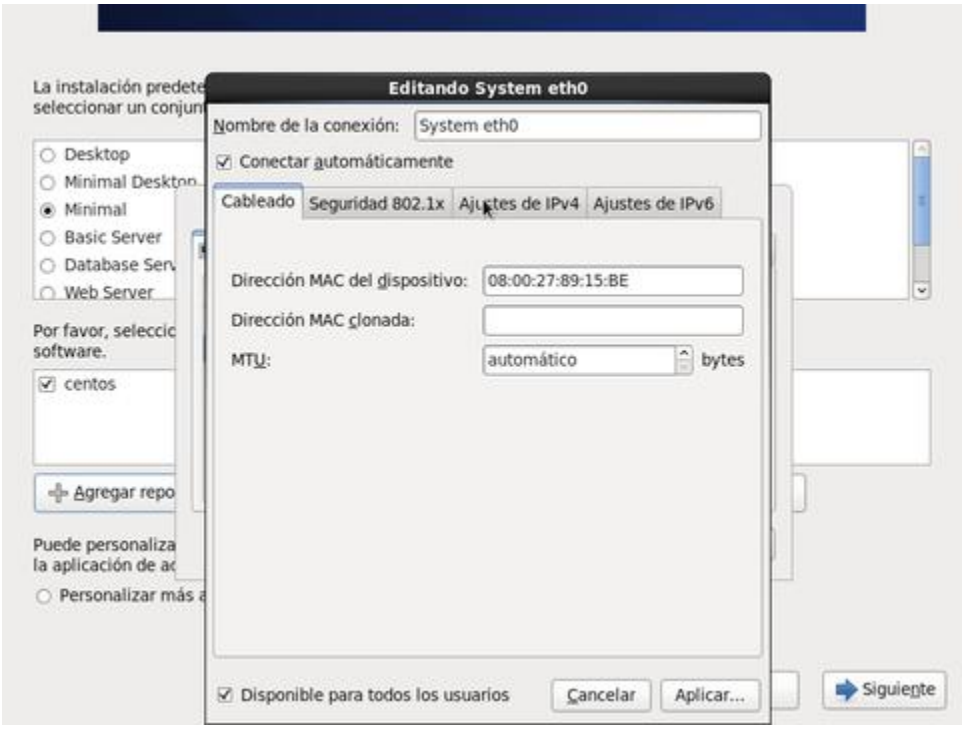
Si dispone de al menos una tarjeta de red, el programa de instalación le solicitará seleccione que dispositivo utilizar para configurar una conexión de red que permita conectarse hacia el URL que especificó en el paso anterior. Una vez seleccionado el dispositivo de red, haga clic sobre el botón denominado **«Aceptar.»**



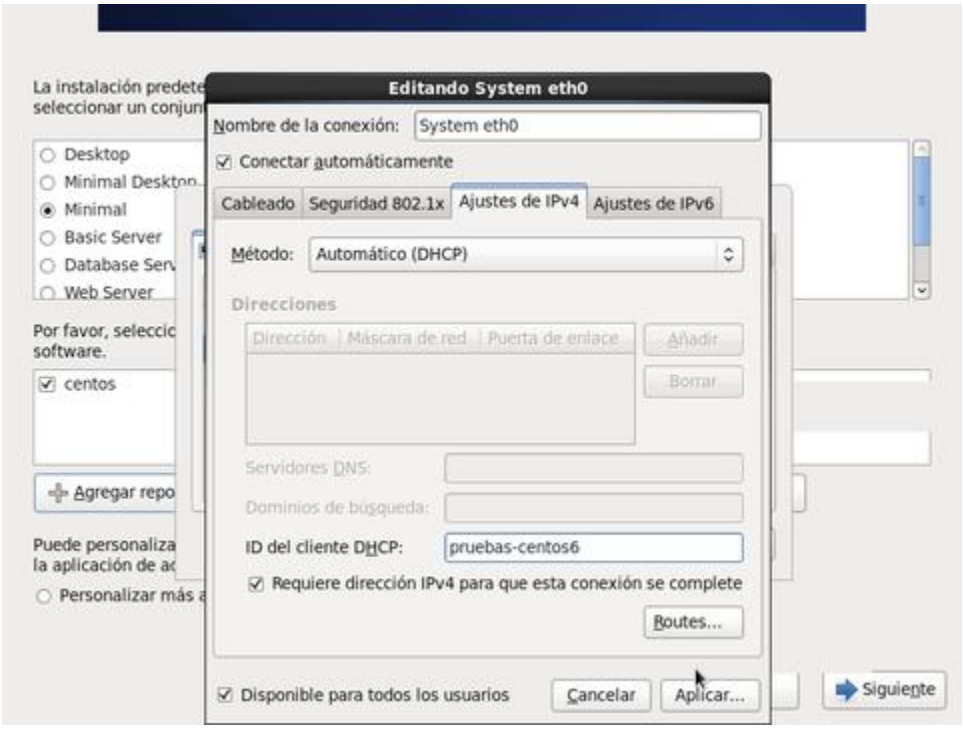
Lo anterior abrirá la ventana **«Conexiones de red»** de NetworkManager. Seleccione la interfaz de red deseada y haga clic sobre el botón denominado **«Editar.»**



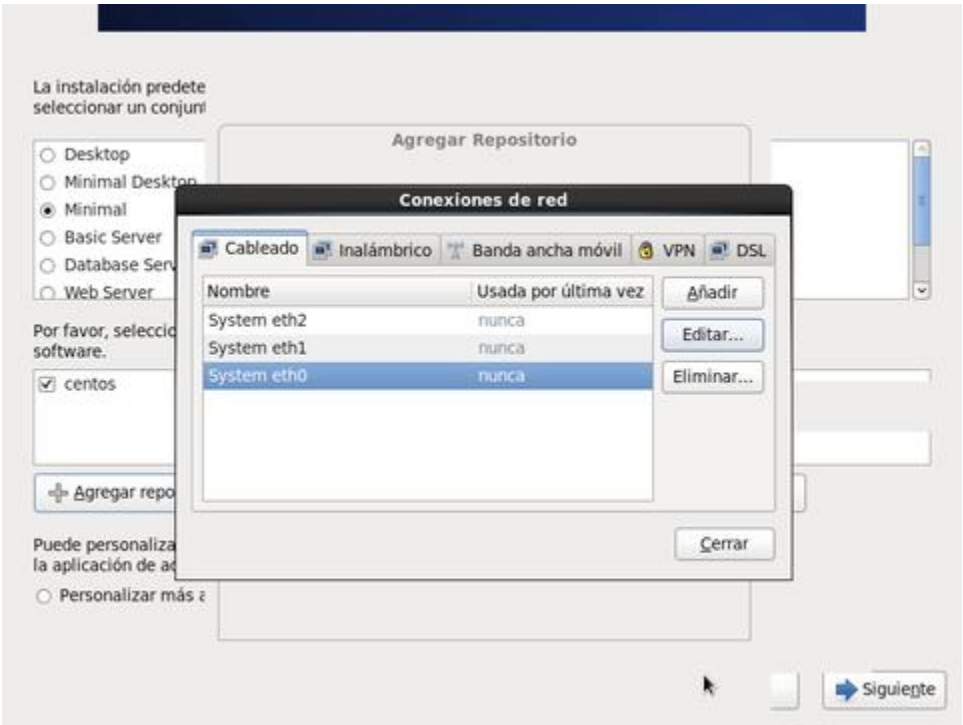
Lo anterior abrirá la ventana de edición de la interfaz. Haga clic sobre la pestaña denominada **«Ajustes de IPv4.»**



Configure los parámetros necesarios para poder establecer una conexión de red. Al terminar, haga clic sobre el botón denominado **«Aplicar.»**

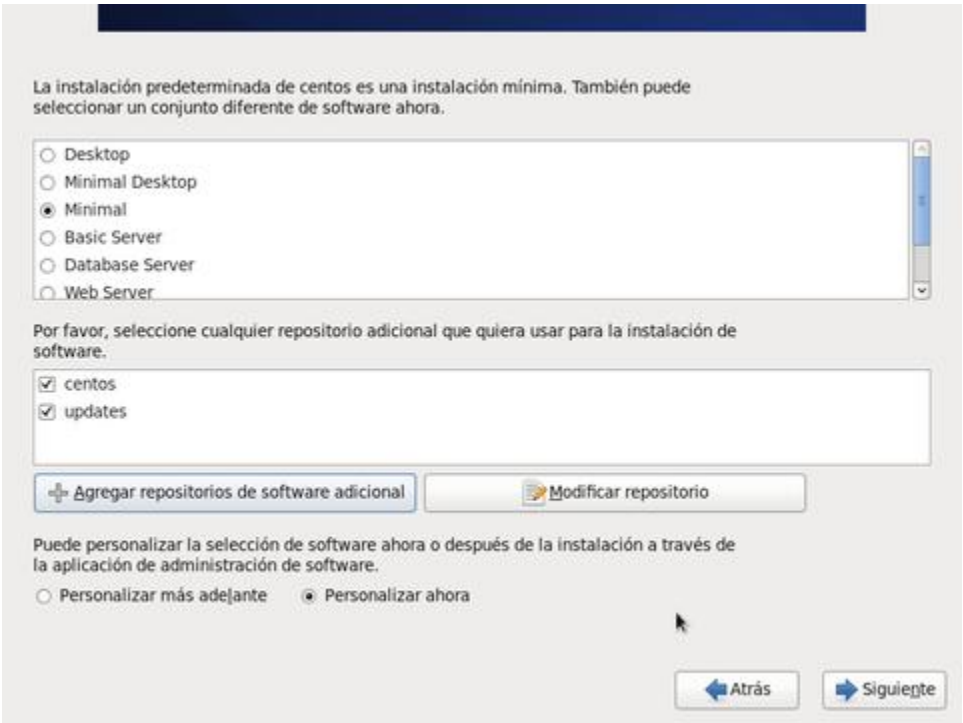


Regresará a la ventana de **«Conexiones de red»**. Haga clic sobre el botón denominado **«Cerrar.»**

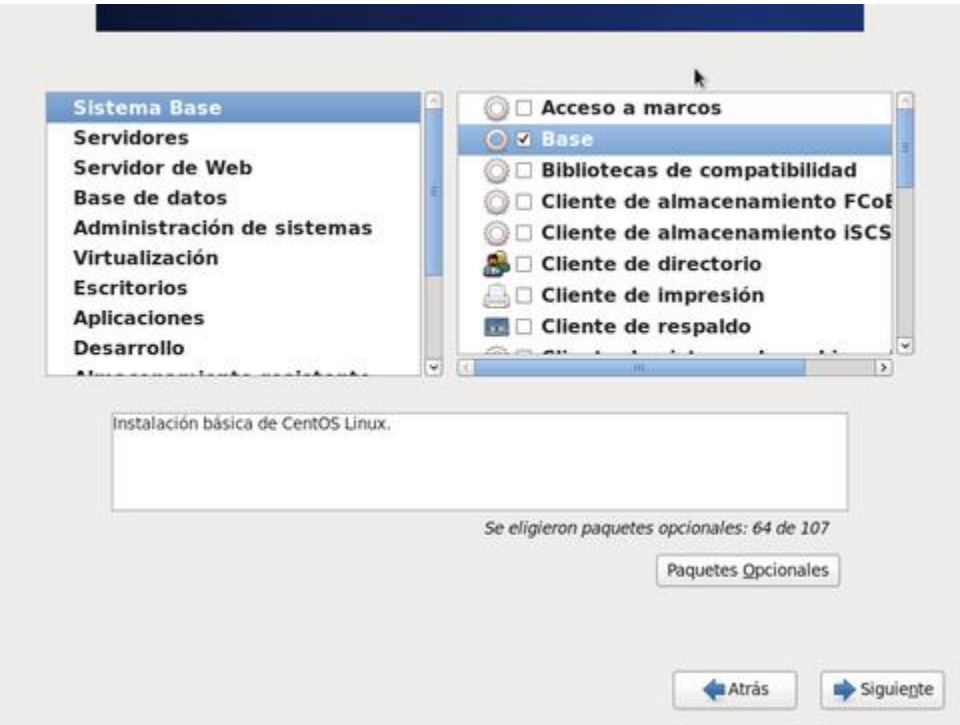


Deberá regresar a la pantalla principal, donde deberá aparecer el almacén YUM que acaba de configurar.

Para elegir grupos específicos de paquetes, haga clic sobre la casilla de opción denominada **«Personalizar ahora.»** Al terminar, haga clic sobre el botón denominado **«Siguiente.»**

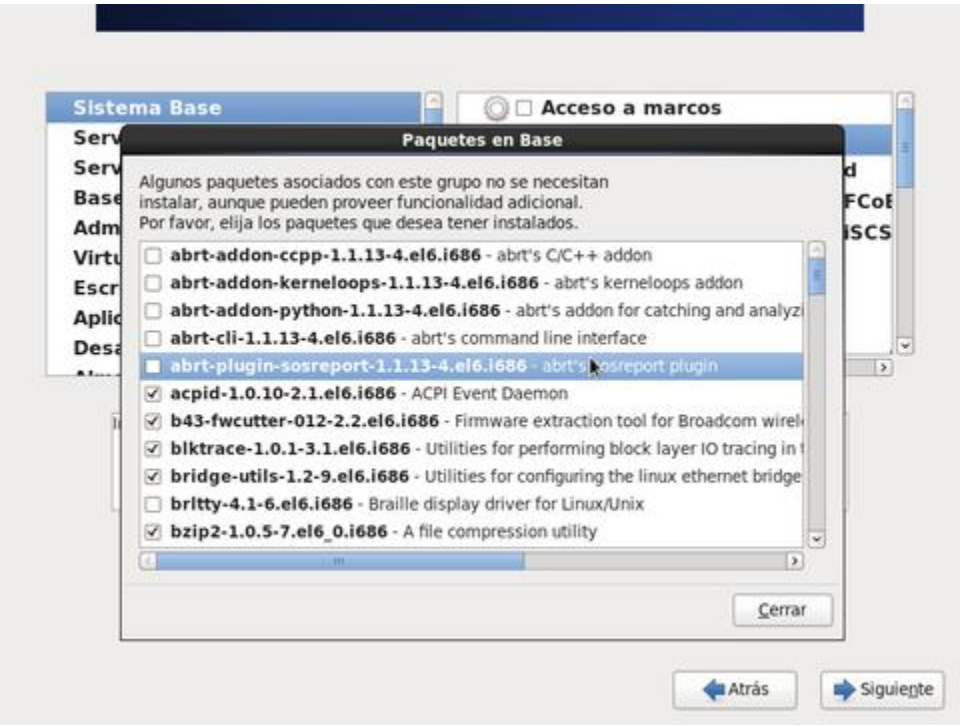


Podrá seleccionar cualquier grupo de paquetes que sirva a necesidades particulares. Prefiera conservar el diseño de **instalación mínima**, y, cuando mucho, añadir el grupo de paquetes denominado **«Base.»**

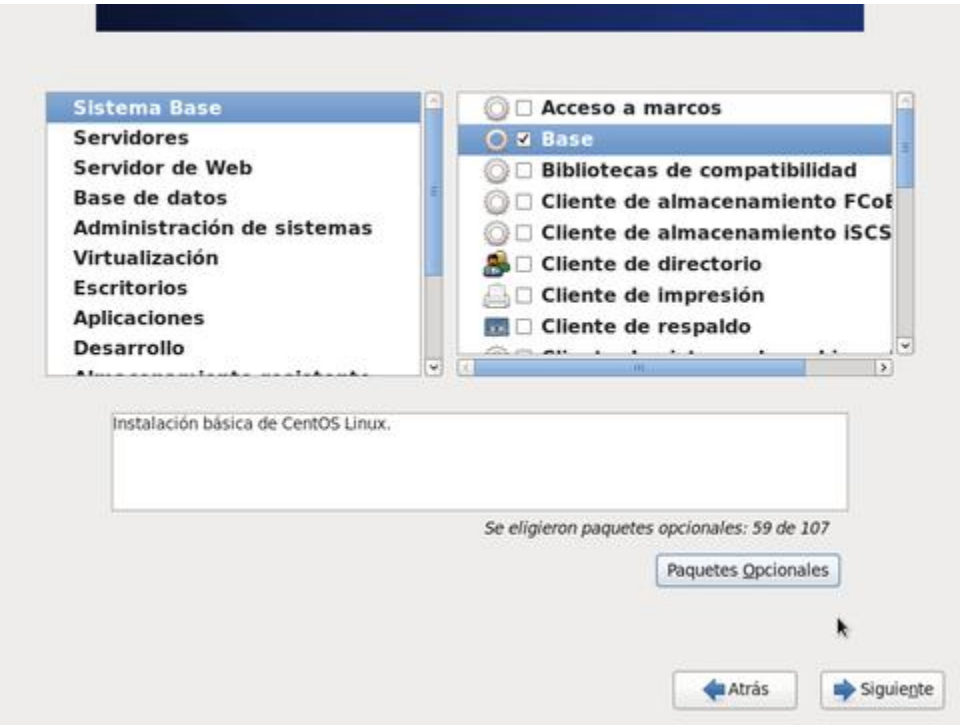


Si posteriormente decide instalar el escritorio gráfico, revise el documento titulado «Ajustes posteriores a la instalación de CentOS 6.»

Si desea personalizar la lista de paquetes que se instalará en un grupo en particular, haga clic sobre el botón denominado **«Paquetes opcionales.»** Ésto abrirá una ventana desde la cual podrá seleccionar lo que requiera y omitir lo que se quiera. Al terminar, haga clic sobre el botón denominado **«Cerrar.»**



Si está conforme y considera que ha terminado de seleccionar los grupos de paquetes, haga clic sobre el botón denominado **«Siguiente.»**



Iniciará el proceso de instalación de paquetes. El tiempo que demore el proceso dependerá de la cantidad de grupos y paquetes que se hayan seleccionado.

Una vez completada la instalación, haga clic sobre el botón **«Reinciar,»** y retire el DVD o disco compacto de la unidad óptica.

3.2. Posterior a la instalación.

Revise el documento titulado «**Ajustes posteriores a la instalación de CentOS 6**.»

4. Ajustes posteriores a la instalación de CentOS 6.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

4.1. Procedimientos.

Una vez terminada la instalación de **CentOS 6** hay varios ajustes que se recomienda realizar.

4.1.1. Nombres de los dispositivos de red.

Las más recientes versiones de **CentOS**, **Fedora™** y **Red Hat™ Enterprise Linux** utilizan un nuevo esquema para los nombres de los dispositivos de red. Los nombres se basan sobre su ubicación física con la finalidad de facilitar su identificación. Los dispositivos de red integrados a la tarjeta madre utilizan el esquema **em[1,2,3,4...]**; los dispositivos PCI utilizan el esquema **p[ranura PCI]p[puerto ethernet]** y —en el caso de dispositivos virtuales— **p[ranura PCI]p[puerto ethernet]_[interfaz virtual]**. Ejemplos:

- em1 corresponde al primer dispositivo de red integrado en la tarjeta madre.
- em2 corresponde al segundo dispositivo de red integrado en la tarjeta madre.
- em3 corresponde al tercer dispositivo de red integrado en la tarjeta madre.
- p1p1 corresponde al primer dispositivo de red en la primera ranura PCI, primer puerto ethernet.
- p2p1 corresponde al primer dispositivo de red en la segunda ranura PCI, primer puerto ethernet.
- p3p1 corresponde al primer dispositivo de red en la tercera ranura PCI, primer puerto ethernet.
- p3p2 corresponde al primer dispositivo de red en la tercera ranura PCI, segundo puerto ethernet.
- p3p2_1 corresponde al primer dispositivo de red en la tercera ranura PCI, segundo puerto ethernet, primer dispositivo virtual.

El nuevo esquema de nombres sólo aplica para sistemas que implementan SMBIOS versión 2.6 y tablas 9 y 41. Puede cotejarse la versión de SMBIOS ejecutando como usuario root el siguiente mandato:

```
biosdecode
```

Pueden determinarse los dispositivos de red presentes en el sistema revisando el contenido del directorio **/sys/class/net/**:

```
ls /sys/class/net/
```

Puede consultarse la asignación de nombres de dispositivos de red presentes en el sistema, a través del archivo /etc/udev/rules.d/70-persistent-net.rules.

```
vi /etc/udev/rules.d/70-persistent-net.rules
```

Si se dispone de SMBIOS 2.6 y tablas 41 y 9, para hacer uso del nuevo esquema de nombres en sistemas que fueron actualizados desde una versión anterior de **CentOS**, **Fedora™** y **Red Hat™ Enterprise Linux**, sólo es necesario eliminar este archivo y reiniciar el sistema.

4.1.2. Dispositivos de red inactivos.

Si realizó la instalación mínima, sin agregar grupos de paquetes al diseño predeterminado o bien sin configurar dispositivos de red o bien lo anterior para para incluir actualizaciones, descubrirá que probablemente los dispositivos de red están desactivados.

Edite los archivos de interfaz de sus dispositivos de red:

```
vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

Asegúrese que al menos una de las interfaces de red tenga el parámetro **«ONBOOT»** con el valor **«yes»**:

```
DEVICE="eth0"
NM_CONTROLLED="yes"
ONBOOT="yes"
HWADDR=08:00:27:89:15:BE
TYPE=Ethernet
BOOTPROTO=dhcp
DEFROUTE=yes
PEERDNS=yes
PEERROUTES=yes
DHCP_CLIENT_ID=pruebas-centos6
IPV4_FAILURE_FATAL=yes
IPV6INIT=no
NAME="System eth0"
UUID=5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03
```

Si el equipo se va a utilizar como servidor, conviene desactivar que la gestión de las interfaces de red se haga a través del servicio **NetworkManager** y dejar que se encargue de ésta el servicio **network**. Cambie **NM_CONTROLLED="yes"**, por **NM_CONTROLLED="no"**:

```
DEVICE="eth0"
NM_CONTROLLED="no"
ONBOOT="yes"
HWADDR=08:00:27:89:15:BE
TYPE=Ethernet
BOOTPROTO=dhcp
DEFROUTE=yes
PEERDNS=yes
PEERROUTES=yes
DHCP_CLIENT_ID=pruebas-centos6
IPV4_FAILURE_FATAL=yes
IPV6INIT=no
NAME="System eth0"
UUID=5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03
```

Para aplicar los cambios, reinicie el servicio **network**:

```
service network restart
```

Cabe señalar que **NetworkManager** sólo está instalado y activo si se instala cualquier entorno de escritorio, pues se trata de un componente esencial para permitir al usuario regular poder gestionar las interfaces de red sin utilizar privilegios de root.

4.1.3. Localización.

Si durante la instalación estableció «Español» como idioma predeterminado, se establecerá la variable de entorno **«LANG»** con el valor **«es_ES.UTF-8,»** lo cual resultará conveniente para los usuarios que radican en España. Sin embargo, ésto hará que en los números las divisiones de miles se hagan con un punto y que la división para decimales se haga con una coma..

Edite el archivo **/etc/sysconfig/i18n**:

```
vi /etc/sysconfig/i18n
```

Localice **LANG="es_ES.UTF-8"**:

```
LANG="es_ES.UTF-8"
SYSFONT="latarcyrheb-sun16"
```

Cambie **LANG="es_ES.UTF-8"** por **LANG="es_MX.UTF-8"** (español de México) o bien la localización que corresponda a su país:

```
LANG="es_MX.UTF-8"
SYSFONT="latarcyrheb-sun16"
```

Edite el archivo **/boot/grub/menu.lst** o bien el archivo **/boot/grub/grub.conf** (el primero es un enlace simbólico que apunta hacia el segundo):

```
vi /boot/grub/menu.lst
```

Localice en éste **LANG=es_ES.UTF-8** (sin comillas):

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/sda2
#          initrd /initrd-[generic-]version.img
#boot=/dev/sda
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
password --md5 $1$xU.tiAbo$5a88IZ2yKPvtdYG5ldAmi/
title centos (2.6.32-279.el6.i686)
        root (hd0,0)
        kernel /vmlinuz-2.6.32-279.el6.i686 ro root=UUID=09c6dc39-a62b-409e-8306-5344640cd104 rd_LVM_L
V=Swap/LogVol00 rd_NO_LUKS rd_NO_MD rd_NO_DM LANG=es_ES.UTF-8 SYSFONT=latarcyrheb-sun16 KEYBOARDTYPE=p
c KEYTABLE=la-latin1 crashkernel=auto rhgb quiet
        initrd /initramfs-2.6.32-279.el6.i686.img
```

Cambie **LANG=es_ES.UTF-8** por **LANG=es_MX.UTF-8** (español de México, sin comillas) o bien la localización que corresponda a su país:

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/sda2
#          initrd /initrd-[generic-]version.img
#boot=/dev/sda
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
password --md5 $1$xU.tiAbo$5a88IZ2yKPvtdYG5ldAmi/
title centos (2.6.32-279.el6.i686)
        root (hd0,0)
        kernel /vmlinuz-2.6.32-279.el6.i686 ro root=UUID=09c6dc39-a62b-409e-8306-5344640cd104 rd_LVM_L
V=Swap/LogVol00 rd_NO_LUKS rd_NO_MD rd_NO_DM LANG=es_MX.UTF-8 SYSFONT=latarcyrheb-sun16 KEYBOARDTYPE=p
c KEYTABLE=la-latin1 crashkernel=auto rhgb quiet
        initrd /initramfs-2.6.32-279.el6.i686.img
```

Reinicie el sistema para que surtan efecto los cambios.

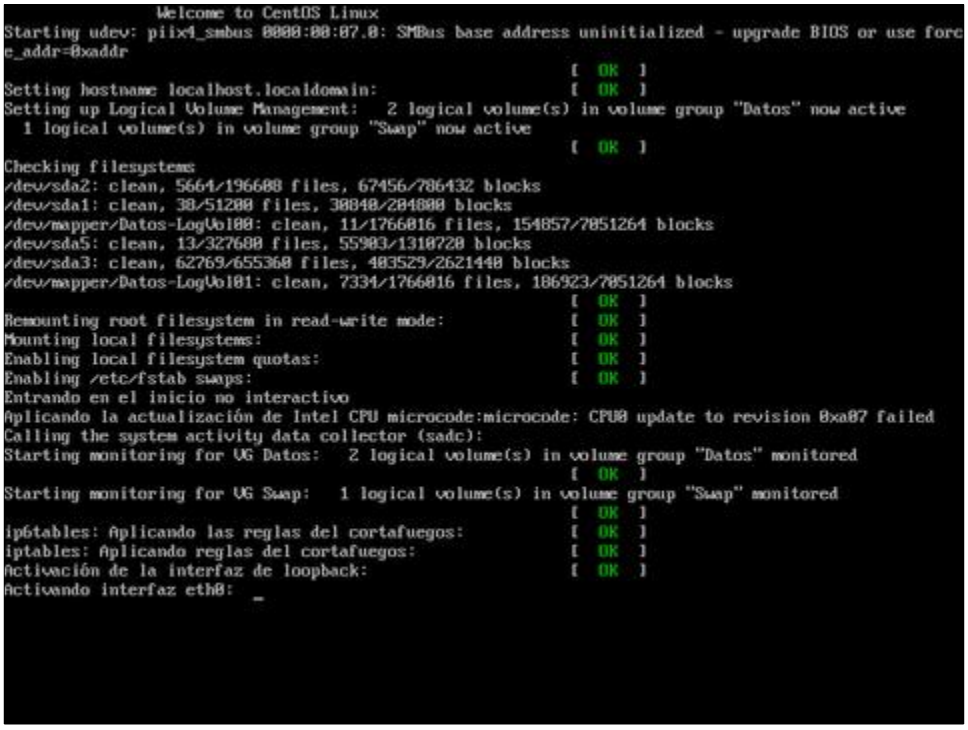
```
reboot
```

4.1.4. Desactivar Plymouth.

Plymouth es la nueva implementación para mostrar un arranque gráfico que tiene como objetivo ocultar de la vista los mensajes de inicio. Si se realizó una instalación mínima, el arranque del sistema se mostrará de la siguiente forma:

Para visualizar qué es lo que ocurre detrás de Plymouth, solo hay que pulsar la tecla **«Supr»** para conmutar al arranque tradicional en texto y viceversa.

En un servidor, probablemente resulte poco conveniente y se prefiera en su lugar un arranque tradicional, mostrando los mensajes de inicio de los servicios.



Edite el archivo **/boot/grub/menu.lst** o bien el archivo **/boot/grub/grub.conf** (el primero es un enlace simbólico que apunta hacia el segundo):

```
vi /boot/grub/menu.lst
```

Localice **rhgb**:

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/sda2
#          initrd /initrd-[generic-]version.img
#boot=/dev/sda
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
password --md5 $1$xU.tiAbo$5a88IZ2yKPvtdYG5ldAmi/
title centos (2.6.32-279.el6.i686)
        root (hd0,0)
        kernel /vmlinuz-2.6.32-279.el6.i686 ro root=UUID=09c6dc39-a62b-409e-8306-5344640cd104 rd_LVM_L
V=Swap/LogVol00 rd_NO_LUKS rd_NO_MD rd_NO_DM LANG=es_MX.UTF-8 SYSFONT=latarcyrheb-sun16 KEYBOARDTYPE=p
c KEYTABLE=la-latin1 crashkernel=auto rhgb quiet
        initrd /initramfs-2.6.32-279.el6.i686.img
```

Elimine la cadena **rhgb**:

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/sda2
#          initrd /initrd-[generic-]version.img
#boot=/dev/sda
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
password --md5 $1$xU.tiAbo$5a88IZ2yKPvtdYG5ldAmi/
title centos (2.6.32-279.el6.i686)
        root (hd0,0)
        kernel /vmlinuz-2.6.32-279.el6.i686 ro root=UUID=09c6dc39-a62b-409e-8306-5344640cd104 rd_LVM_L
V=Swap/LogVol00 rd_NO_LUKS rd_NO_MD rd_NO_DM LANG=es_MX.UTF-8 SYSFONT=latarcyrheb-sun16 KEYBOARDTYPE=p
c KEYTABLE=la-latin1 crashkernel=auto quiet
        initrd /initramfs-2.6.32-279.el6.i686.img
```

Reinicie el sistema para que surtan efecto los cambios:

```
reboot
```

4.1.5. Instalar y habilitar, el modo gráfico.

Si considera que requiere utilizar el modo gráfico, omita la sección anterior (Desactivar Plymouth) e instale los siguientes grupos de paquetes:

```
yum -y groupinstall x11 basic-desktop general-desktop
```

Complemente instalando algunos paquetes de herramientas de administración.

```
yum -y install system-config-services system-config-date \
    system-config-printer system-config-lvm \
    system-config-language system-config-keyboard \
    cups-pk-helper policycoreutils-gui
```

Nota.

Probablemente quiera eliminar los siguientes paquetes, que solo son útiles para realizar depuración del núcleo y enviar reportes de errores de las aplicaciones gráficas a los desarrolladores de CentOS.

```
yum remove kexec-tools abrt-*
```

Luego, hay que editar el archivo **/etc/inittab**.

```
vi /etc/inittab
```

Al final del archivo, localice la siguiente línea:

```
id:3:initdefault:
```

Y reemplazar en ésta el **3** por un **5**:

```
id:5:initdefault:
```

Guarde el archivo, salga del editor de texto

Instale el complemento para GDM (el gestor de pantalla de GNOME), con la finalidad de que los mensajes de error que se pudieran generar al arrancar el sistema, se muestren con icono de advertencia en la pantalla gráfica de autenticación:

```
yum -y install plymouth-gdm-hooks
```

Ejecute lo siguiente para instalar y establecer, el tema gráfico predeterminado de CentOS 6 (rings) para Plymouth:

```
yum -y install plymouth-theme-rings
plymouth-set-default-theme rings
/usr/libexec/plymouth/plymouth-update-initrd
```

Si desea un tema más atractivo y vistoso, establezca el tema solar:

```
yum -y install plymouth-theme-solar
plymouth-set-default-theme solar
/usr/libexec/plymouth/plymouth-update-initrd
```

Nota.

Plymouth solo se mostrará si el sistema dispone de una tarjeta de gráficos con soporte para **KMS** (**K**ernel **m**ode-**s**etting) en el núcleo de Linux o bien definiendo manualmente una resolución como parámetro de inicio del núcleo de Linux (ejemplo: vga=0x315 activará la resolución a 800x600, vga=0x317 activará una resolución de 1024x768).

Reinicie el sistema para que apliquen los cambios e inicie en modo gráfico.

```
reboot
```

4.1.6. Ajustar la zona horaria, fecha y hora del sistema.

Verifique si hay actualizaciones para el paquete **tzdata** antes de realizar cualquier procedimiento:

```
yum -y update tzdata
```

La zona horaria generalmente se establece desde el programa de instalación. Si requiere ajustarla, primero consulte el contenido del directorio **/usr/share/zoneinfo** y descienda a los subdirectorios en el interior hasta encontrar la zona horaria apropiada para su localidad.

```
ls /usr/share/zoneinfo
```

Edite el archivo **/etc/sysconfig/clock** y consulte que zona horaria se estableció:

```
vi /etc/sysconfig/clock
```

Asumiendo que su localidad es la Ciudad de México, el contenido debe ser similar al siguiente:

```
ZONE="America/Mexico City"
```

Cambie el valor de la variable ZONE a la que corresponda a su localidad.

A fin de evitar problemas posteriores, respalde el archivo **/etc/localtime** utilizado por el sistema:

```
cp /etc/localtime /etc/localtime.bak
```

Copie el archivo de zona que corresponde a su localidad sobre-escribiendo al archivo **/etc/localtime**. En el siguiente ejemplo se sobre-escribirá el archivo **/etc/localtime** con el archivo **/usr/share/zoneinfo/America/Mexico_City**:

```
cp /usr/share/zoneinfo/America/Mexico_City /etc/localtime
```

Para determinar cuál es la fecha y hora actual del sistema, ejecute el mandato **date** sin opciones ni argumentos:

```
date
```

Lo anterior debe devolver una salida similar a la siguiente:

```
dom abr 28 15:26:30 CDT 2013
```

El ajuste manual del la hora del sistema puede realizarse a través del mandato **date** con la opción -s (set o establecer) la siguiente sintaxis:

```
date -s "[día] [MES] [año] [hora]:[minuto]:[segundos]"
```

En el siguiente ejemplo se establecerá la hora y fecha del sistema a las 15:30:00 del 19 de mayo de 2013:

```
date -s "19 MAY 2013 15:30:00"
```

Si desea establecer la **fecha y hora exacta** del sistema, instale primero el paquete **ntp**:

```
yum -y install ntp
```

Ejecute el mandato **ntpdate** utilizando cualquier servidor NTP como argumento:

```
ntpdate 0.pool.ntp.org
```

Lo anterior debe devolver una salida similar a la siguiente:

```
28 Apr 15:45:29 ntpdate[29180]: adjust time server 132.248.30.3 offset -0.023721 sec
```

Para que el sistema siempre esté a la hora exacta, active e inicie el servicio **ntpd**:

```
chkconfig ntpd on && service ntpd start
```

Una vez iniciado el servicio **ntpd**, para realizar el ajuste manual de la fecha y hora del sistema debe ejecutar el mandato **ntpdate** con la opción -u para utilizar un puerto aleatorio distinto al 123/UDP y cualquier servidor NTP como argumento:

```
ntpdate -u 0.pool.ntp.org
```

Para más detalles respecto del protocolo NTP y el mandato **ntpdate**, consulte el documento titulado Configuración y uso de NTP.

5. Planificadores de Entrada/Salida en Linux.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

5.1. Introducción.

La planificación de Entrada/Salida (*Input/Output Scheduling* o *I/O scheduling*) consiste en el método mediante el cual los sistemas operativos deciden el orden en que se procesan las peticiones de lectura/escritura en el disco duro o unidad de almacenamiento. El objetivo de optimizar el sistema, eligiendo un algoritmo de planificación de Entrada/salida, es disminuir los tiempos de búsqueda (*seek times*), priorizar las peticiones de ciertos procesos de Entrada/salida, asignar un ancho de banda más adecuado a cada procesos o garantizar que algunas peticiones se atenderán antes de una fecha de caducidad. Básicamente, fueron diseñados para mitigar la demora de los tiempos de búsqueda que utilizan el brazo y el cabezal, de los disco duros, para moverse desde una posición, hacia otra posición más alejada.

La mayoría de los planificadores de Entrada/Salida (*I/O schedulers*) se basan sobre el **algoritmo del elevador**, el cual determina el movimiento del brazo de un disco y cabezal al servir peticiones de lectura/escritura. Este algoritmo basa su nombre sobre el comportamiento del elevador de un edificio, donde éste continúa su trayectoria actual hacia arriba o hacia abajo hasta que éste se vacía por completo, deteniéndose solo para permitir que nuevos individuos lo aborden, siempre que éstos vayan en la misma dirección actual del elevador.

5.2. Planificadores de Entrada/Salida disponibles en el núcleo de Linux.

5.2.1. Anticipatory.

Consiste en un algoritmo cuyo objetivo es incrementar la eficiencia de la utilización del disco duro, *anticipando* las operaciones sincrónicas de lectura. Fue el planificador de Entrada/Salida del núcleo de Linux desde la versión 2.6.0 hasta a versión 2.6.18. Desde la versión 2.6.33, fue eliminado del núcleo de Linux, debido a que hoy en día hay muy pocas unidades de almacenamiento basadas sobre los estándares **SCSI-1** y **IDE/ATA** y que aún estén en operación.

Era ideal para servidores HTTP o sistemas de Escritorio, con discos duros **SCSI-1** o **IDE/ATA**, pues se conseguía un rendimiento sensiblemente superior.

Funciona realizando una demora controlada antes de despachar los procesos de Entrada/Salida, con la finalidad de agregar o re-ordenar las operaciones de búsqueda que son realizadas, mejorando el desempeño y reduciendo de manera significativa las operaciones de petición de los discos duros. Está diseñado específicamente para optimizar los sistemas con sub-sistemas de discos pequeños o bien muy lentos, como es el caso de discos duros con estándar SCSI-1 y algunos antiguos modelos de IDE/ATA.

Es totalmente inadecuado para discos duros que utilicen **TCQ** (***T**agged **C**ommand **Q**ueuing*), que es una tecnología consiste en la optimización de peticiones de lectura/escritura desde la propia unidad de disco duro, permitiendo al sistema operativo realizar múltiples peticiones de lectura/escritura. Esta tecnología es utilizada en los discos duros con el estándar SCSI-2, PATA y SATA, es decir todos los modernos disco duros que actualmente existen en mercado. Es totalmente inapropiado para unidades de almacenamiento de alto desempeño, así como con arreglos de discos por RAID.

Asumiendo que se dispone de un disco duro basado sobre el estándar SCSI-1 o bien IDE/ATA, que se ha asignado como el dispositivo **/dev/sda**, este planificador de Entrada/Salida puede aplicarse de manera inmediata ejecutando:

```
echo "anticipatory" > /sys/block/sda/queue/scheduler
```

Lo anterior hará que el sistema utilice este planificador de Entrada/Salida hasta el siguiente reinicio. Verifique que realmente se ha establecido como el planificador de Entrada/Salida actual ejecutando lo siguiente:

```
cat /sys/block/sda/queue/scheduler
```

Lo cual debe devolver una salida similar a la siguiente:

```
[anticipatory] noop deadline cfq
```

Para que el cambio sea permanente, se debe editar el archivo **/boot/grub/menu.lst**:

```
vi /boot/grub/menu.lst
```

Y añadir a los parámetros de inicio del núcleo el parámetro **elevator**, con el valor **anticipatory**.

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/sda2
#          initrd /initrd-[generic-]version.img
#boot=/dev/sda
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
password --md5 $1$xU.tiAbo$5a88IZ2yKPvtdYG5ldAmi/
title centos (2.6.32-279.el6.i686)
        root (hd0,0)
        kernel /vmlinuz-2.6.32-279.el6.i686 ro root=UUID=09c6dc39-a62b-409e-8306-5344640cd104 rd_LVM_L
V=Swap/LogVol00 rd_NO_LUKS rd_NO_MD rd_NO_DM LANG=es_MX.UTF-8 SYSFONT=latarcyrheb-sun16 KEYBOARDTYPE=p
c KEYTABLE=la-latin1 crashkernel=auto rhgb quiet elevator=anticipatory
        initrd /initramfs-2.6.32-279.el6.i686.img
```

5.2.2. CFQ.

CFQ, que es el acrónimo de ***C**ompletely **F**air **Q**ueuing*, que podría traducirse como *encolado de procesamiento completamente justo*, es el planificador de Entrada/Salida predeterminado de CentOS y Red Hat Enterprise Linux. Ofrece un excelente rendimiento para la mayoría de los usos que se le pueda dar al sistema operativo.

Su objetivo es mantener una cola de procesamiento de Entrada/Salida escalable por proceso e intentar distribuir equitativamente el ancho de banda disponible para los procesos de Entrada/Salida, entre todas las peticiones de Entrada/Salida.

Funciona colocando peticiones sincrónicas, enviadas por un proceso, dentro de un número de colas de procesamiento por proceso y luego distribuyendo intervalos de tiempo para cada una de las colas de procesamiento, a fin de que puedan acceder al disco duro.

La longitud de los intervalos de tiempo, así como también el número de peticiones que tiene permitido una cola de procesamiento, depende de la prioridad del mismo procesos de Entrada/Salida. De este modo, las peticiones asincrónicas para todos los procesos son agrupadas y procesadas, en menos colas de procesamientos, asignando una por prioridad.

Técnicamente, tiene el mismo efecto similar al del planificador Anticipatory, manteniendo una buena capacidad de procesamiento, al permitir que las colas de procesamiento puedan pausar al finalizar un procesos de Entrada/Salida, *anticipando* el procesos de Entrada/Salida más cercano de ese mismo proceso.

Puede verificar que CFQ es el planificador de Entrada/Salida utilizado por el sistema, ejecutando lo siguiente:

```
cat /sys/block/sda/queue/scheduler
```

Lo cual debe devolver una salida similar a la siguiente:

```
[cfq] anticipatory noop deadline
```

Para utilizar este planificador de Entrada/Salida, es innecesario hacer modificación alguna, pues es el predeterminando del sistema.

5.2.3. Deadline.

Funciona de modo similar al tiempo real, utilizando una política de asignación en circuito (*round robin*), para intentar distribuir equitativamente las peticiones de Entrada/Salida, evitando se agote la capacidad de procesamiento.

Básicamente impone tiempos de caducidad (*deadline*) a todas las operaciones de Entrada/Salida, con la finalidad de impedir que se agote la capacidad de recibir peticiones. Utiliza cinco colas de procesamiento, dos de las cuales son ordenadas de acuerdo a los tiempos de caducidad, al mismo tiempo que las colas de procesamiento son ordenadas de acuerdo a su número de sector.

Antes de servir la siguiente petición, decide que cola de procesamiento utilizar, otorgando mayor prioridad a las peticiones de lectura, verificando después si ha caducado la primera petición en la cola de procesamiento.

De modo predeterminado, los tiempos de caducidad son de 500 ms para las peticiones de lectura y de 5 segundos para las peticiones de escritura.

Se recomienda su uso para servidores dedicados para bases de datos y particularmente para aquellos sistemas que disponen de discos duros con capacidad de **TCQ**, así como en sistemas con unidades de almacenamiento de alto desempeño, es decir discos duros con el estándar SCSI-2, PATA o SATA

Asumiendo que se dispone de un disco duro o unidad de almacenamiento, que se ha asignado como el dispositivo **/dev/sda**, este planificador de Entrada/Salida puede aplicarse de manera inmediata ejecutando:

```
echo "deadline" > /sys/block/sda/queue/scheduler
```

Lo anterior hará que el sistema utilice este planificador de Entrada/Salida hasta el siguiente reinicio. Verifique que realmente se ha establecido como el planificador de Entrada/Salida actual ejecutando:

```
cat /sys/block/sda/queue/scheduler
```

Lo cual debe devolver una salida similar a la siguiente:

```
[deadline] anticipatory noop cfq
```

Para que el cambio sea permanente, se debe editar el archivo **/boot/grub/menu.lst**:

```
vi /boot/grub/menu.lst
```

Y añadir a los parámetros de inicio del núcleo el parámetro **elevator**, con el valor **deadline**.

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/sda2
#          initrd /initrd-[generic-]version.img
#boot=/dev/sda
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
password --md5 $1$xU.tiAbo$5a88IZ2yKPvtdYG5ldAmi/
title centos (2.6.32-279.el6.i686)
        root (hd0,0)
        kernel /vmlinuz-2.6.32-279.el6.i686 ro root=UUID=09c6dc39-a62b-409e-8306-5344640cd104 rd_LVM_L
V=Swap/LogVol00 rd_NO_LUKS rd_NO_MD rd_NO_DM LANG=es_MX.UTF-8 SYSFONT=latarcyrheb-sun16 KEYBOARDTYPE=p
c KEYTABLE=la-latin1 crashkernel=auto rhgb quiet elevator=deadline
        initrd /initramfs-2.6.32-279.el6.i686.img
```

5.2.4. Noop.

Es el planificador de Entrada/Salida más simple que existe. Funciona insertando todas las peticiones de Entrada/Salida dentro de una cola de procesamiento tipo **FIFO** (***f****irst* ***i****n,* ***f****irst* ***o****ut*, que se traduce como *primero en entrar, primero en salir*) e implementando fusión de peticiones.

Asume que la optimización del desempeño de Entrada/Salida será gestionado por otro nivel de la jerarquía de Entrada/Salida, como pudiera ser en el dispositivo de bloque o bien un **HBA** (**H**ost **B**us **A**dapter o adaptador de transporte del anfitrión) inteligente, como en el caso en los controladores RAID para SAS (***S****erial*** *A****ttached*** *S****CSI***) o bien un controlador conectado de manera externa, como ocurre con los **SAN** (***S****torage* ***A****rea* ***N****etwork* o Redes de Área de Almacenamiento).

Este planificador de Entrada/Salida es principalmente utilizado con unidades de estado sólido (**SSD**, **S**olid **S**tate **D**rives) basadas sobre memoria Flash, NAND o SDRAM y en dispositivos que carecen de dependencia a movimientos mecánicos, los cuales carecen de re-ordenamiento de peticiones múltiples de Entrada/Salida, donde se agrupan juntas las peticiones de Entrada/Salida que están físicamente cercanas, reduciendo el tiempo de petición y la variabilidad del tiempo de servicio de Entrada/Salida.

Asumiendo que se dispone de un disco duro o unidad de almacenamiento, que se ha asignado como el dispositivo **/dev/sda**, este planificador de Entrada/Salida puede aplicarse de manera inmediata ejecutando:

```
echo "noop" > /sys/block/sda/queue/scheduler
```

Lo anterior hará que el sistema utilice este planificador de Entrada/Salida hasta el siguiente reinicio. Verifique que realmente se ha establecido como el planificador de Entrada/Salida actual ejecutando:

```
cat /sys/block/sda/queue/scheduler
```

Lo cual debe devolver una salida similar a la siguiente:

```
[noop] anticipatory deadline cfq
```

Para que el cambio sea permanente, se debe editar el archivo **/boot/grub/menu.lst**:

```
vi /boot/grub/menu.lst
```

Y añadir a los parámetros de inicio del núcleo el parámetro **elevator**, con el valor **noop**.

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/sda2
#          initrd /initrd-[generic-]version.img
#boot=/dev/sda
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
password --md5 $1$xU.tiAbo$5a88IZ2yKPvtdYG5ldAmi/
title centos (2.6.32-279.el6.i686)
        root (hd0,0)
        kernel /vmlinuz-2.6.32-279.el6.i686 ro root=UUID=09c6dc39-a62b-409e-8306-5344640cd104 rd_LVM_L
V=Swap/LogVol00 rd_NO_LUKS rd_NO_MD rd_NO_DM LANG=es_MX.UTF-8 SYSFONT=latarcyrheb-sun16 KEYBOARDTYPE=p
c KEYTABLE=la-latin1 crashkernel=auto rhgb quiet elevator=noop
        initrd /initramfs-2.6.32-279.el6.i686.img
```

5.3. ¿Cuál planificador de Entrada/Salida elegir?

Depende del tipo de unidad(es) de almacenamiento, servicios utilizados en el sistema, capacidades de procesamiento y los tipos de procesos que se quieran priorizar.

En general, se puede utilizar:

- **anticipatory** en equipos con discos duros viejos (**SCSI-1** o **IDE/ATA**).
- **cfq** se recomienda en sistemas para uso general o bien se desconoce qué hacer. Es el planificador predeterminado.
- **deadline** en servidores con unidades de almacenamiento PATA, SATA, SCSI-2 y unidades sin **HBA** inteligente.
- **noop** se recomienda en sistemas con unidades de estado sólido basadas sobre memoria Flash, NAND, SDRAM, máquinas virtuales o bien sistemas con unidades de almacenamiento controladas por **HBA** inteligentes — como en los casos de Serial SCSI o un SAN.

Se recomienda realizar pruebas de desempeño y de rendimiento, antes de elegir el planificador de Entrada/salida definitivo para un sistema en particular. Elija el que se considere que funcione mejor.

5.4. Bibliografía.

- https://secure.wikimedia.org/wikipedia/en/wiki/Elevator_algorithm
- https://secure.wikimedia.org/wikipedia/es/wiki/Planificaci%C3%B3n_de_E/S
- https://secure.wikimedia.org/wikipedia/en/wiki/Anticipatory_scheduling
- https://secure.wikimedia.org/wikipedia/en/wiki/CFQ
- https://secure.wikimedia.org/wikipedia/en/wiki/Deadline_scheduler
- https://secure.wikimedia.org/wikipedia/en/wiki/Noop_scheduler
- https://www.redhat.com/magazine/008jun05/features/schedulers/

6. Uso del disco de rescate de CentOS 6.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org/

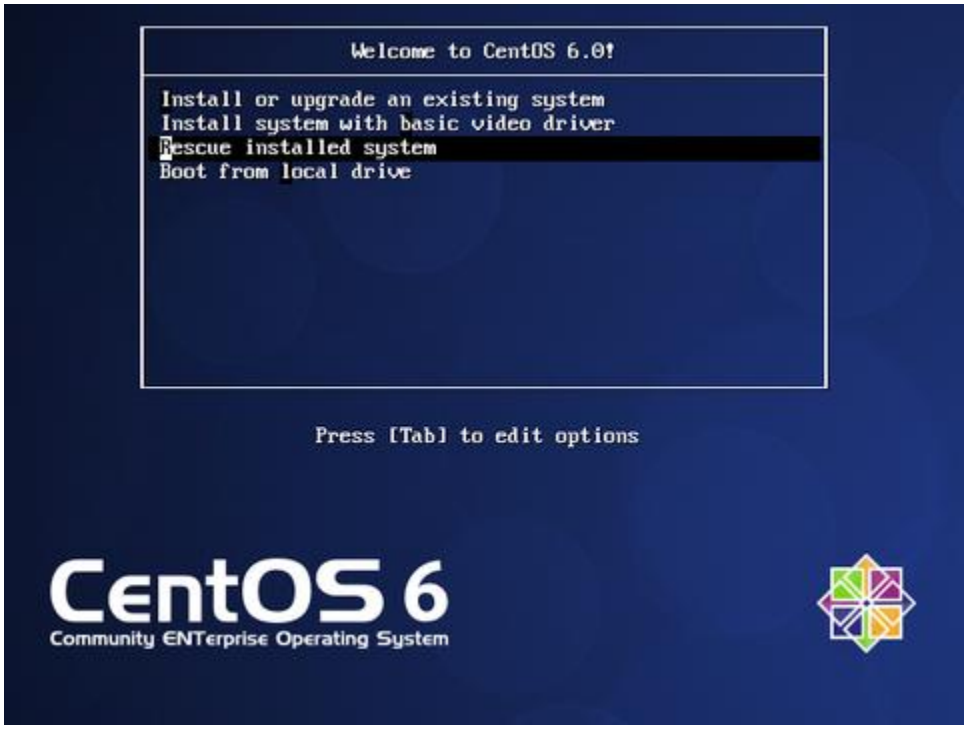
Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

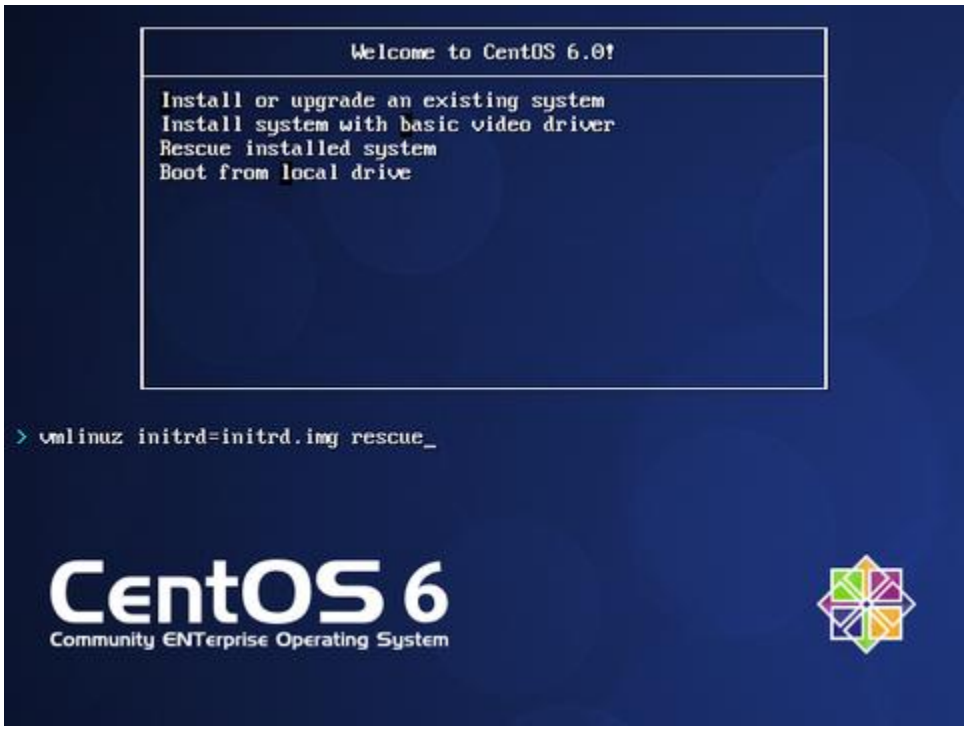
6.1. Procedimientos.

Inicie el sistema con el disco de instalación. En cuanto aparezca la pantalla de bienvenida, pulse cualquiera de la tecla ↑ o bien la tecla ↓. Tendrá sólo 60 segundos para hacerlo.

Seleccione la entrada denominada **«Rescue installed system.»**



Puede pulsar la tecla ↵ (**ENTER**) y continuar. Si desea ver que opciones de arranque utiliza esta entrada, pulse la tecla **TAB**. Notará que la opción de arranque es simplemente **rescue**. Pulse la tecla ↵ (**ENTER**) para proceder.



El disco de instalación iniciará en modo rescate. Lo primero a configurar es el idioma.

Seleccione **Spanish**, pulse la tecla **TAB** hasta que resalte **Ok** y pulse la tecla ↵ (**ENTER**).

A partir de este punto, todos los mensajes se mostrarán al español.

Si su teclado tiene disposición Español/España, seleccione **es**, pulse la tecla **TAB** hasta que resalte **Aceptar** y pulse la tecla ↵ (**ENTER**).

Si su teclado tiene disposición Español/Latinoamérica, seleccione **la-latin1**, pulse la tecla **TAB** hasta que resalte **Aceptar** y pulse la tecla ↵ (**ENTER**).

Seleccione **CD/DVD Local**, pulse la tecla **TAB** hasta que resalte **Aceptar** y pulse la tecla ↵ (**ENTER**).

Se le preguntará si desea activar las tarjetas de red del sistema. Pulse la tecla **TAB** hasta que resalte **Si** o bien **No** y pulse la tecla ↵ (**ENTER**).

Si respondió con **Si** en la pantalla anterior, el sistema le solicitará que elija qué tarjeta o bien tarjetas, desea utilizar para establecer una conexión de red. Utilice la tecla **ESPACIO** para definir activar los dispositivos de red y pulse la tecla **TAB** para conmutar entre los elementos de pantalla. Configure lo necesario para establecer la conexión de red por DHCP o bien por dirección IP fija. Una vez terminado lo anterior, pulse la tecla **TAB** hasta que resalte **Aceptar** y pulse la tecla ↵ (**ENTER**).

Tiene cuatro opciones a elegir.

- **Continuar**. El entorno de rescate intentará encontrar una instalación de GNU/Linux en el disco duro e intentará montar todas las particiones en el árbol que corresponde, debajo del directorio **/mnt/sysimage**. De este modo se podrá acceder en modo lectura y escritura al sistema de archivos y así poder realizar los cambios o modificaciones que requiera.
- **Modo lectura**. Similar a la opción anterior, pero todo el sistema de archivos se montará en modo de sólo lectura.
- **Omitir**. Se omitirá el montado del sistema de archivos del disco duro. Esta opción es idónea para realizar reparaciones del sistema de archivos de las particiones, utilizando el mandato **fsck** o bien para realizar operaciones que requieren que las particiones estén sin montar.
- **Avanzado**. Permitirá hacer uso de dispositivos especiales de almacenamiento, como Redes de Área de Almacenamiento (SAN), es decir FCoE, iSCSI y zFCP.

Seleccione **Continuar** y pulse la tecla ↵ (**ENTER**).

El sistema examinará los dispositivos de almacenamiento. Ésto puede demorar varios segundos.

Una vez detectada la instalación en el disco duro, el entorno de rescate le informará que las particiones de la instalación existente de GNU/Linux estarán montadas debajo del directorio **/mnt/sysimage**. Para continuar, pulse la tecla ↵ (**ENTER**).

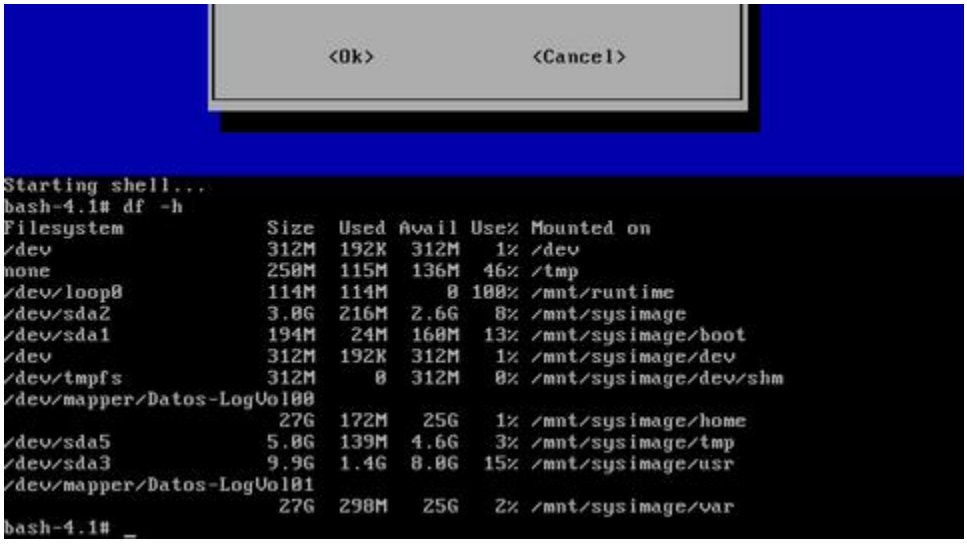
Aparecerá una pantalla con tres opciones.

- **Start shell**. Iniciará el intérprete de mandatos, desde el cual podrá trabajar de modo similar al nivel de ejecución 1 (mono usuario) y tendrá acceso a un conjunto básico de herramientas de diagnóstico y reparación.
- **Run diagnostic**. Ejecutará **FirstAidKit**, una herramienta que realiza verificación y reparación, automática de algunos problemas comúnes.
- **Reboot**. Reiniciará el sistema.

Seleccione **Start shell** y pulse la tecla ↵ (**ENTER**).

Lo anterior le devolverá un intérprete de mandatos.

Verifique que todas las particiones de la instalación de GNU/Linux han sido montadas, utilizado el mandato **df** con la opción **-h**.



Ejecute el mandato exit para regresar a la pantalla anterior.

Nota.

Si ejecuta el siguiente mandato:

```
chroot /mnt/sysimage
```

Cambiará del sistema operativo del disco de rescate, al sistema operativo en el disco duro.

Ésto puede ser de mucha ayuda para, por mencionar un ejemplo, cambiar la clave de acceso del usuario root, para lo cual sólo se requiere ejecutar el mandato **passwd** sin argumentos:

```
passwd
```

O bien también es posible reinstalar manualmente el gestor de arranque del sistema ejecutando lo siguiente, asumiendo que la unidad de almacenamiento corresponde al dispositivo **/dev/sda**:

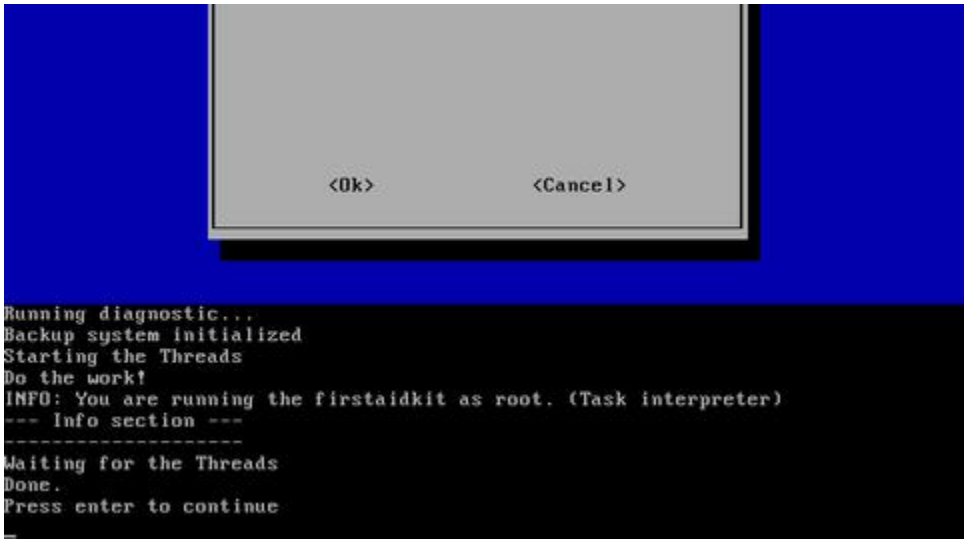
```
grub-install /dev/sda
```

Para regresar al sistema operativo del entorno de rescate, ejecute el mandato **exit**.

```
exit
```

Si lo desea, puede seleccionar ejecutar **fakd**, es decir FirstAidKit, que es una herramienta de diagnóstico para verificación y reparación automática, del gestor de arranque, imagen de disco RAM para el inicio del sistema (*initrd*), arreglos de discos por *software* y re-instalación de algunos paquetes básicos.

Si hay algo que reparar, **FirstAidKit** lo hará de manera automática. Pulse la tecla ↵ (**ENTER**) para salir y regresar a la pantalla anterior.



Seleccione **Reboot** y pulse la tecla ↵ (**ENTER**) para reiniciar el sistema.

Retire el DVD o disco compacto de la unidad óptica.

7. Iniciando el sistema en nivel de ejecución 1 (nivel mono-usuario).

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

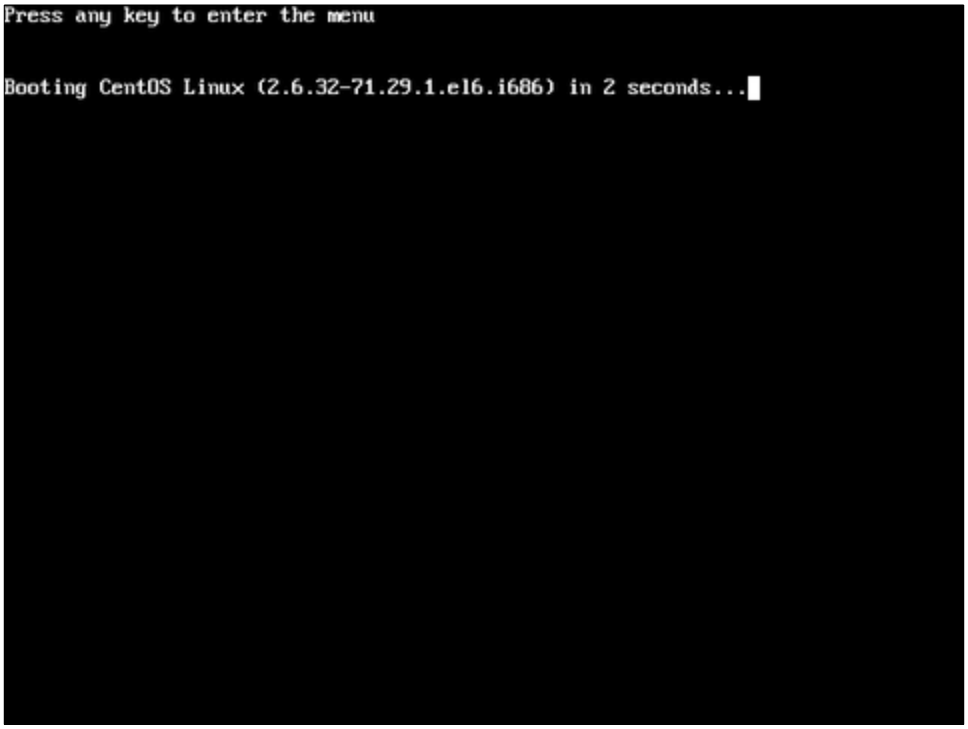
© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

7.1. Introducción

Existen situaciones en las cuales se puede requerir iniciar el sistema en nivel de ejecución 1, también denominado **nivel monousuario**, a fin de realizar tareas de mantenimiento o bien para realizar correcciones y otros ajustes.

7.2. Procedimientos.

Al iniciar el sistema, éste presentará la pantalla del gestor de arranque, conocido como **GRUB** (**Gr**and **U**nified **B**oot Loader). Pulse cualquier tecla, **excepto** la tecla **ENTER**, para detener la cuenta regresiva de 3 segundos y poder ingresar al menú de **GRUB**.

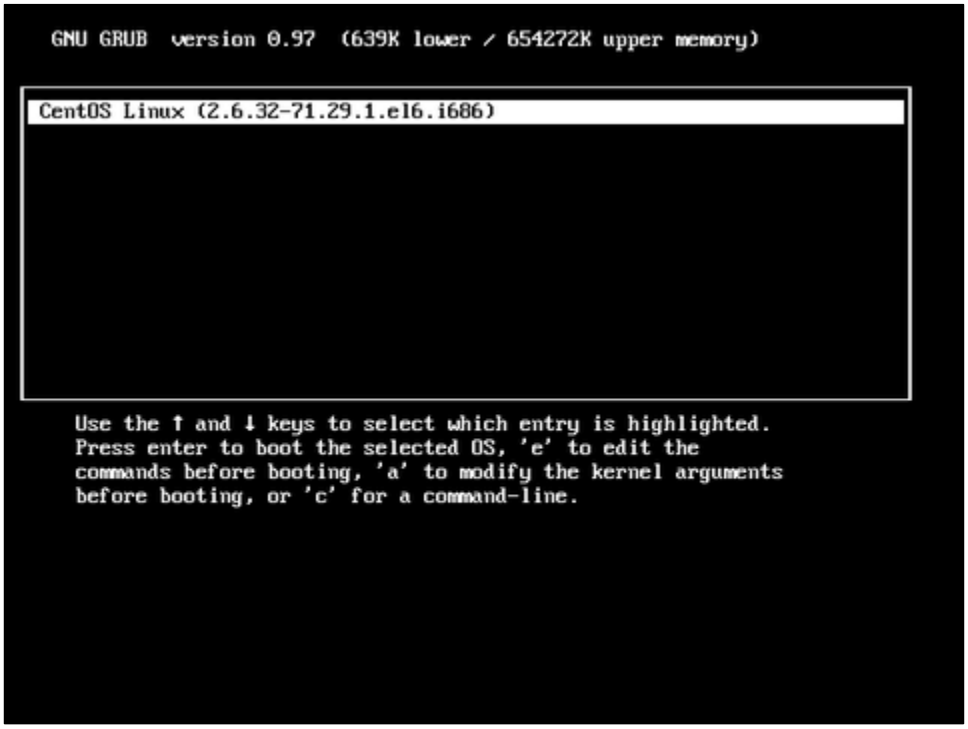


Si durante la instalación de CentOS, **se definió una clave de acceso para el gestor de arranque**, aparecerá la siguiente pantalla.

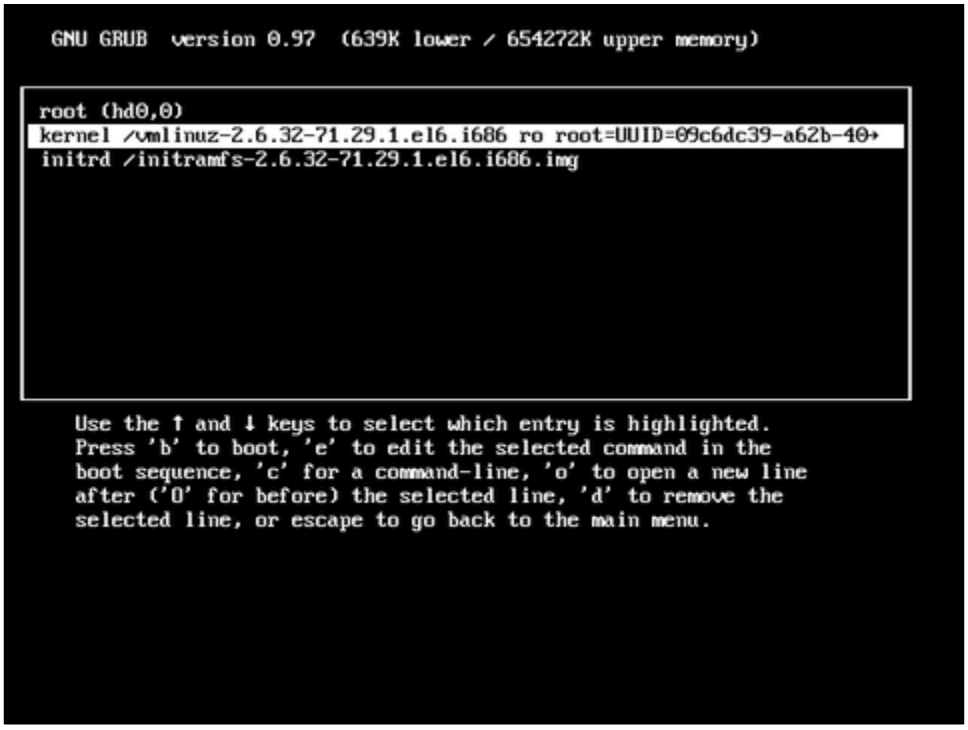
Para ingresar la clave de acceso, pulse la tecla **«p»**.

Ingrese la clave de acceso que se asignó al gestor de arranque durante la instalación del sistema operativo:

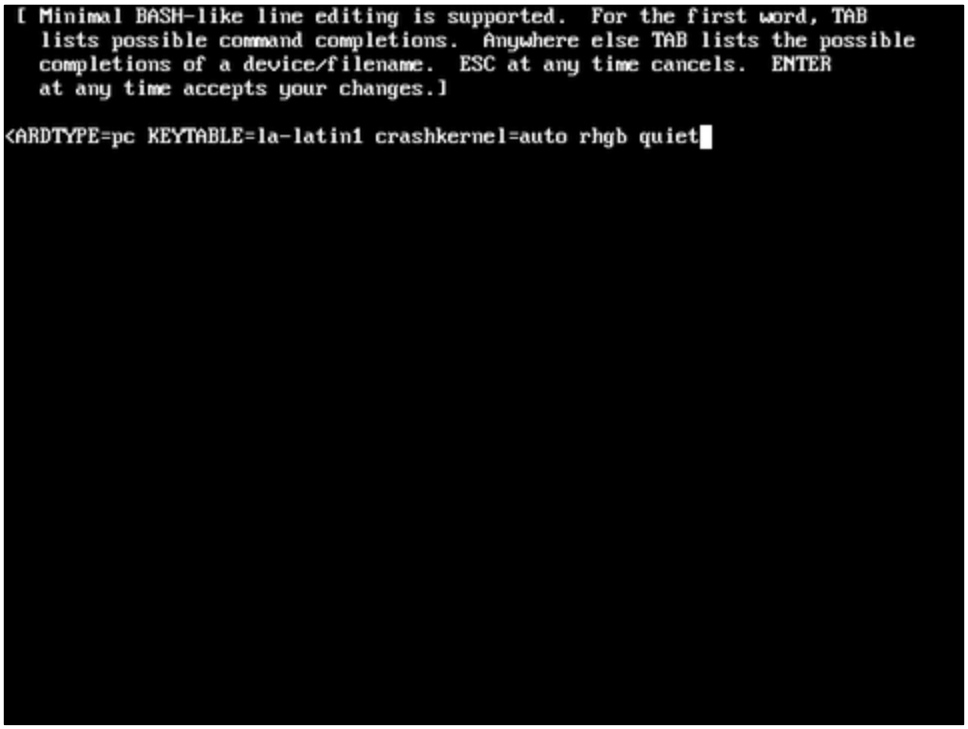
El texto de la sección de opciones cambiará después de ingresar la clave de acceso. Pulse la tecla **«e»** para editar las opciones de arranque del núcleo seleccionado:



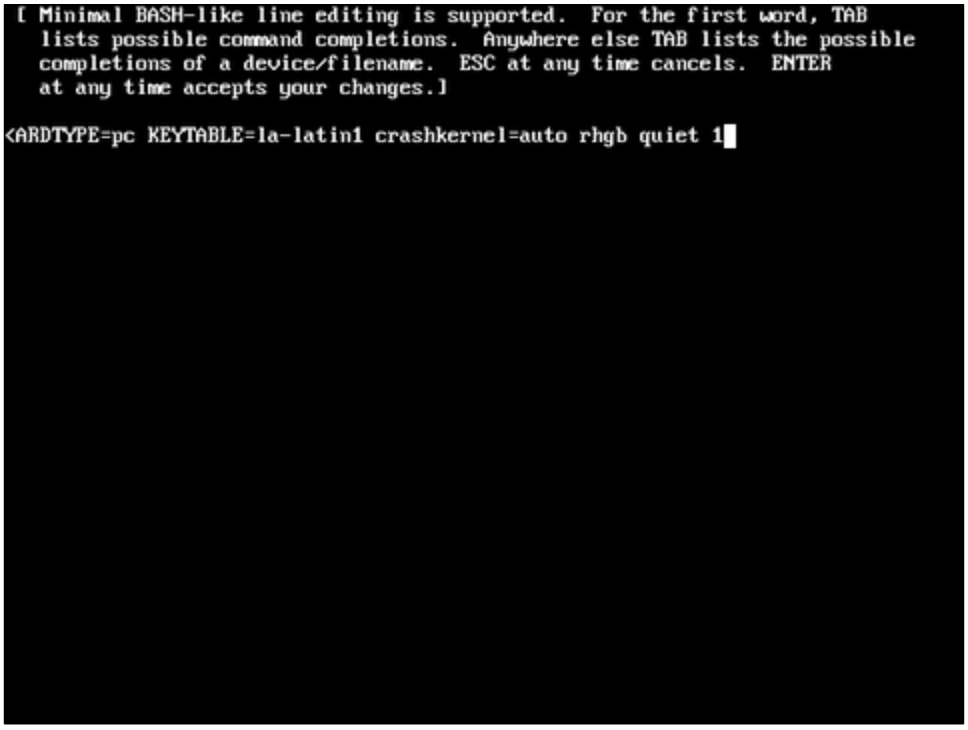
Seleccione la línea referente al núcleo.



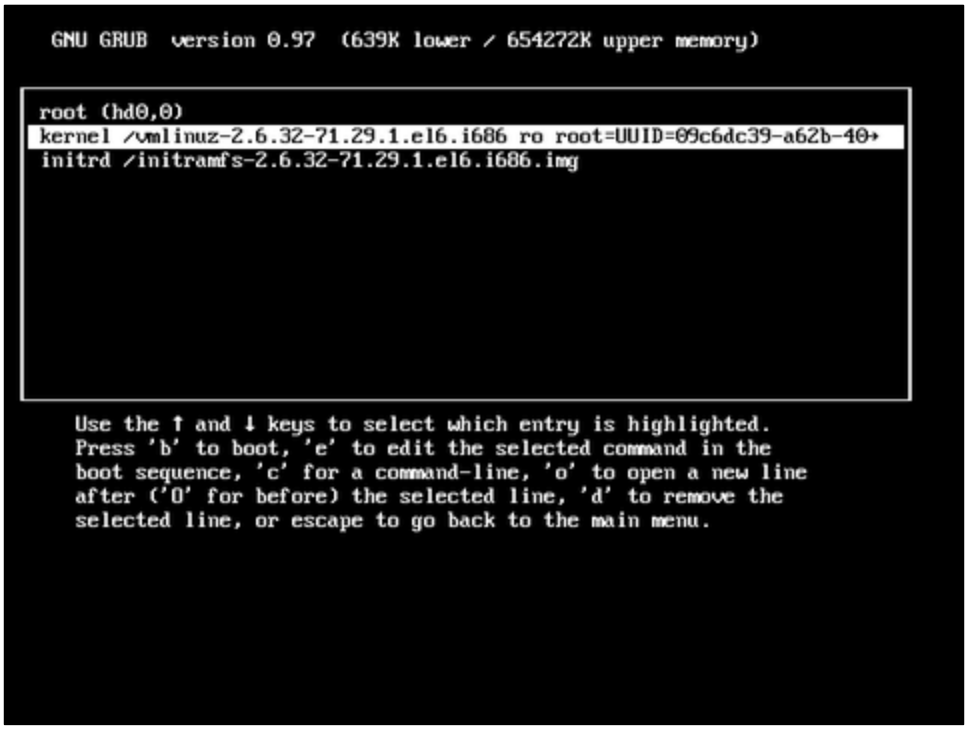
Con el fin de realizar una edición de esta línea, vuelva a pulsar la tecla **«e»**. Se mostrará la siguiente pantalla



Agregue un espacio y un número 1, al final de la línea y pulse la tecla **ENTER**.



Regresará a la pantalla anterior.



Pulse la tecla **«b»**. Ésto hará que el sistema inicie en nivel de ejecución 1:

Informando a INIT para ir a modo monousuario.
init: rc main process (844) killed by TERM signal
[root@localhost /]# _

8. Gestión de servicios.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales **(incluyendo su publicación, a través de cualquier medio, por entidades con fines de lucro)**. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en castellano. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

8.1. Introducción.

La gestión de servicios consiste en activar o desactivar servicios en los distintos niveles de ejecución del sistema y en iniciar, detener o activar éstos cuando las circunstancias lo requieran. Este documento describe los procedimientos correspondientes en CentOS, Fedora™, Red Hat™ Enterprise Linux, openSUSE™ y SUSE™ Linux Enterprise.

8.2. Niveles de ejecución.

GNU/Linux tiene 7 niveles de ejecución:

- 0: Apaga el sistema.
- 1 o S: Nivel mono-usuario.
- 2: Multi-usuario, sin unidades de almacenamiento remoto o sin conexión de red.
- 3: Multi-usuario, con unidades de almacenamiento remoto.
- 4: Experimental.
- 5: Multi-usuario con servidor de video.
- 6: Reinicia sistema.

Los servicios del sistema utilizan los niveles de ejecución 2, 3, 4 y 5. Los niveles de ejecución 0, 1 y 6 están reservados para los usos descritos arriba.

Para verificar el nivel de ejecución predeterminado del sistema, puede consultarse el contenido del archivo **/etc/inittab**, ejecutando lo siguiente:

```
cat /etc/inittab |grep initdefault |grep id
```

Lo anterior debe devolver algo similar a lo siguiente:

```
id:5:initdefault:
```

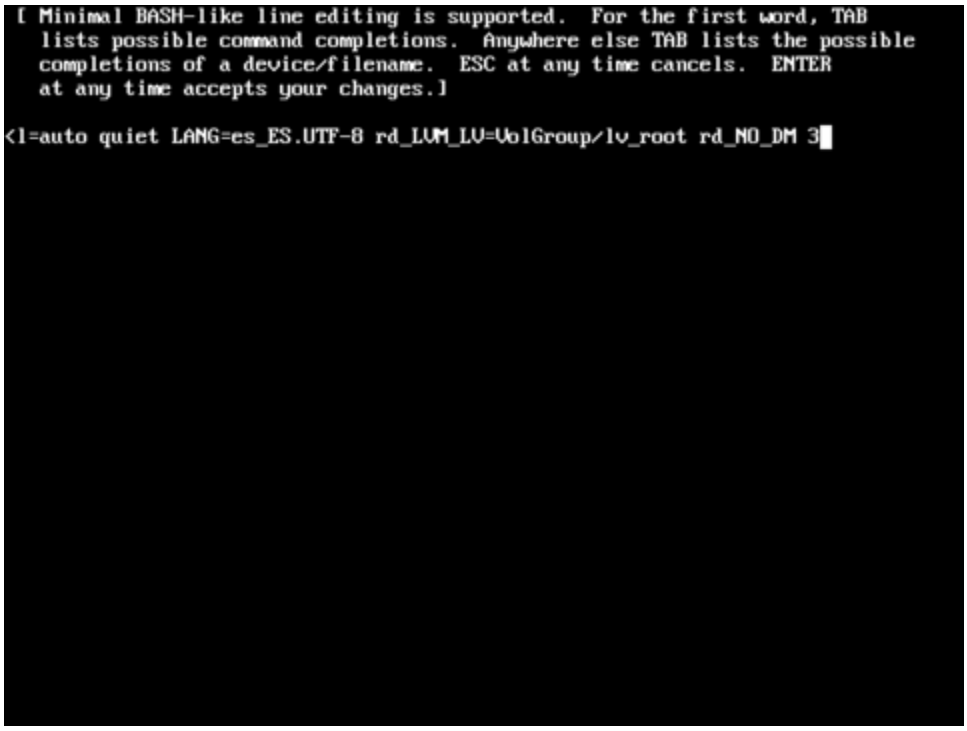
Lo anterior indica que el nivel de ejecución predeterminado del sistema es el 5. Para cambiar el valor del nivel de ejecución predeterminado, sólo es necesario editar como root el archivo **/etc/inittab**:

```
vim /etc/inittab
```

Y reemplazar el número que esté establecido, por el de cualquier otro nivel de ejecución deseado, entre 1 y 5. **¡Jamás se debe establecer 0 (apagar) o 6 (reiniciar)!**

Para que surta efecto el cambio, se reinicia el sistema, el cual deberá utilizar, de modo predeterminado, el nivel de ejecución especificado en el archivo **/etc/inittab**.

También es posible iniciar el sistema en cualquier nivel de ejecución distinto al definido en el archivo **/etc/inittab**, sin necesidad de modificar archivo alguno, añadiendo el número correspondiente como argumento de arranque del núcleo desde el gestor de arranque del sistema.



Inicio en nivel de ejecución 3 desde el gestor de arranque de CentOS 6.

Inicio en nivel de ejecución 3 desde el gestor de arranque de openSUSE™ 11.

Para verificar el nivel de ejecución actual, se utiliza el mandato **runlevel**.

```
runlevel
```

Cuando la salida devuelve la letra N mayúscula y un número, significa que el sistema inició en ese nivel de ejecución y que es inexistente un nivel de ejecución previo. En el siguiente ejemplo de salida, se indica que el sistema está en el nivel de ejecución 5, sin niveles de ejecución previos:

```
N 5
```

Cuando la salida del mandato **runlevel** es de dos números, el primer número corresponde al nivel de ejecución previo y el segundo corresponde al nivel de ejecución actual. En el siguiente ejemplo, se indica que el sistema está en el nivel de ejecución 5 y que anteriormente se estaba en el nivel de ejecución 3:

```
3 5
```

Para obtener un poco más de detalle, también puede utilizarse el mandato **who** con la opción -r.

```
who -r
```

En el siguiente ejemplo, la salida muestra que el nivel de ejecución es el 5 y que el último nivel de ejecución fue el 3.

```
     run-level 5  Jun 27 17:09          last=3
```

Para conmutar de inmediato de nivel de ejecución, iniciando o terminando los servicios que sean necesarios, se ejecuta el mandato **init**, utilizando como argumento el número de nivel al que se desea cambiar. En el siguiente ejemplo, se conmuta al nivel de ejecución 1:

```
init 1
```

En el siguiente ejemplo, se conmuta al nivel de ejecución 3:

```
init 3
```

En el siguiente ejemplo, se conmuta al nivel de ejecución 6, el cual reinicia el sistema:

```
init 6
```

En el siguiente ejemplo, se conmuta al nivel de ejecución 0, el cual apaga el sistema:

```
init 0
```

Para conmutar el nivel de ejecución indicando al mandato **init** cuánto esperará entre los envíos a los procesos de las señales SIGTERM y SIGKILL, se utiliza el mandato **telinit**. De modo predeterminado son 5 segundos y con la opción -t se puede establecer un valor distinto en segundos.

Cada uno de los niveles de ejecución dispone de un sub-directorio dentro del directorio /etc. En el caso de CentOS, Fedora™ y Red Hat™ Enterprise Linux, se utilizan los siguientes directorios:

- /etc/rc.d/rc0.d
- /etc/rc.d/rc1.d
- /etc/rc.d/rc2.d
- /etc/rc.d/rc3.d
- /etc/rc.d/rc4.d
- /etc/rc.d/rc5.d
- /etc/rc.d/rc6.d

En el caso de openSUSE™ y SUSE™ Linux Enteprise, también existen estas mismas rutas, pero son enlaces simbólicos de los siguientes directorios, pudiendo trabajarse con unos u otros de manera indistinta:

- /etc/init.d/rc0.d
- /etc/init.d/rc1.d
- /etc/init.d/rc2.d
- /etc/init.d/rc3.d
- /etc/init.d/rc4.d
- /etc/init.d/rc5.d
- /etc/init.d/rc6.d

Cada uno de estos directorios incluye enlaces simbólicos que apuntan hacia los guiones de arranque de los servicios, los cuales están dentro del directorio **/etc/init.d/**. Hay dos tipos de enlaces, los que inician el servicio y los que terminan el servicio. Ambos tipos de enlaces incluyen un número que determina la prioridad de inicio o de terminación de un servicio respecto de otros servicios en el sistema.

Liste el contenido del directorio **/etc/rc.d/rc3.d** ejecutando lo siguiente:

```
ls /etc/rc.d/rc3.d
```

El siguiente ejemplo es una muestra de lo que **podría** contener el directorio **/etc/rc.d/rc3.d**:

```
K01avahi-dnsconfd   K69rpcsvcgssd      K87rpcbind       S23NetworkManager
K10saslauthd        K72autofs          K88iscsi         S24avahi-daemon
K10zvbid            K73slapd           K89iscsid        S24nslcd
K15atd              K73ypbind          K89rdisc         S25cups
K30sendmail         K74nscd            K90network       S25netfs
K30vboxweb-service  K75ntpdate         K92ip6tables     S26haldaemon
K35nmb              K80fcoe            K92iptables      S50bluetooth
K35smb              K80lldpad          K95firstboot     S58ntpd
K36xrdp             K83nfslock         S02lvm2-monitor  S60vsftpd
K50dnsmasq          K83rpcgssd         S11portreserve   S90crond
K50netconsole       K83rpcidmapd       S12rsyslog       S95atd
K50snmpd            K84wpa_supplicant  S13cpuspeed      S99rc-local
K50snmptrapd        K87multipathd      S15mdmonitor
K60nfs              K87restorecond     S22messagebus
```

Un servicio que tenga un enlace simbólico denominado **S80algo**, significa que el servicio iniciará después de todos los demás servicios que tengan un número menor. Es decir, **S80algo** iniciará después de **S70otro**.

Un servicio que tenga un enlace simbólico denominado **K30algo**, significa que el servicio terminará antes que todos los demás servicios que tengan un número mayor. Es decir, **K30algo** terminará primero que **K40otro**.

Para que un servicio esté activo, debe tener un enlace simbólico denominado **S**[*nn*X] (donde **S** significa **S**tart, *nn* es el número de prioridad, que puede ir de 00 a 99 y X el nombre del servicio) dentro de los directorios de los niveles de ejecución 2, 3, 4 y 5. Estos enlaces simbólicos se acompañan de un enlace K[*nn*X] en los niveles de ejecución 0, 1, 6 y aquellos donde el servicio esté desactivado, para poder terminar normalmente el servicio involucrado.

Para que un servicio esté inactivo, debe tener un enlace simbólico denominado **K**[*nn*X] (donde **K** significa **K**ill, *nn* es el número de prioridad, que puede ir de 00 a 99 y X el nombre del servicio) dentro de los directorios de los niveles de ejecución 2, 3, 4 y 5 y deben estar ausentes los enlaces denominados S[*nn*X].

Todas las distribuciones de GNU/Linux funcionan de este modo.

La ausencia de los enlaces simbólicos de inicio, aquellos cuyo nombre inicia con S mayúscula, en alguno de los directorios que corresponden a los niveles de ejecución, significa que dicho servicio está inhabilitado en ese nivel de ejecución. La presencia de un enlace simbólico de terminación, aquellos cuyo nombre inicia con K mayúscula, en cualquiera de niveles de ejecución (generalmente, al menos 0, 1 y 6), significa que el servicio está desactivado. Por ejemplo, si se tiene el servicio **sshd** y éste tiene los siguientes enlaces:

```
/etc/rc.d/rc0.d/K25sshd
/etc/rc.d/rc1.d/K25sshd
/etc/rc.d/rc2.d/S55sshd
/etc/rc.d/rc3.d/S55sshd
/etc/rc.d/rc4.d/S55sshd
/etc/rc.d/rc5.d/S55sshd
/etc/rc.d/rc6.d/K25sshd
```

Lo anterior significaría que el servicio **sshd** está habilitado en los niveles de ejecución 2, 3, 4 y 5 y que se termina al conmutar a los niveles de ejecución 0, 1 y 6.

Si se tuviera el siguiente escenario:

```
/etc/rc.d/rc0.d/K25sshd
/etc/rc.d/rc1.d/K25sshd
/etc/rc.d/rc2.d/K25sshd
/etc/rc.d/rc3.d/S55sshd
/etc/rc.d/rc4.d/K25sshd
/etc/rc.d/rc5.d/S55sshd
/etc/rc.d/rc6.d/K25sshd
```

Lo anterior significaría que el servicio **sshd** sólo estaría activo en los niveles de ejecución 3 y 5. Si se conmuta a cualquier otro nivel (0, 1, 2, 4 o 6), el servicio es detenido por el sistema. Si por ejemplo se estuviese trabajando en el nivel de ejecución 5 y se conmuta al nivel de ejecución 3, el servicio seguiría funcionando sin ser afectado. Si en cambio se está en el nivel de ejecución 5 y se conmuta al nivel de ejecución 2, donde hay un enlace de terminación de servicio, el servicio es detenido.

Si se tuviera el siguiente escenario:

```
/etc/rc.d/rc0.d/K25sshd
/etc/rc.d/rc1.d/K25sshd
/etc/rc.d/rc2.d/S55sshd
/etc/rc.d/rc3.d/K25sshd
/etc/rc.d/rc3.d/S55sshd
/etc/rc.d/rc4.d/K25sshd
/etc/rc.d/rc5.d/K25sshd
/etc/rc.d/rc5.d/S55sshd
/etc/rc.d/rc6.d/K25sshd
```

Lo anterior significaría que el servicio **sshd** sería reiniciado si se conmuta hacia los niveles 3 o 5, pues existen tanto los enlaces de inicio como los de terminación en los directorios de los niveles de ejecución 3 y 5. Conmutar hacia cualquier otro nivel de ejecución detendría el servicio.

Si se tuviera el siguiente escenario:

```
/etc/rc.d/rc0.d/K25sshd
/etc/rc.d/rc1.d/K25sshd
/etc/rc.d/rc2.d/S55sshd
/etc/rc.d/rc3.d/K25sshd
/etc/rc.d/rc3.d/S55sshd
/etc/rc.d/rc4.d/K25sshd
/etc/rc.d/rc5.d/S55sshd
/etc/rc.d/rc6.d/K25sshd
```

Conmutar desde el nivel de ejecución 5 hacia el nivel de ejecución 3 reiniciaría el servicio. Conmutar desde el nivel de ejecución 3 hacia el nivel de ejecución 5, tendría nulo efecto sobre el servicio, a menos que el servicio **sshd** hubiese sido detenido previamente, en cuyo caso hubiese sido iniciado.

Cada archivo de inicio de servicio, que se encuentran dentro del directorio **/etc/init.d/**, incluye como mínimo la siguiente información, comentada con almohadillas:

```
#Interprete de mandatos utilizado
#
#nombre del servicio       Descripción breve del servicio
#
#chkconfig: niveles de ejecución en los que estás activo el servicio y
#           los números de prioridad de inicio y terminación, respectivamente,
#           con los que serán creados los enlaces simbólicos en cada nivel
#           de ejecución.
#
#description: Descripción detallada del servicio.

### BEGIN INIT INFO
# Provides: componentes que son provistos por el servicio
# Required-Start: requisitos para iniciar el servicio
# Required-Stop: requisitos para detener el servicio
# Default-Start:  niveles de ejecución en los que está activo el servicio
# Default-Stop: niveles de ejecución en los que está inhabilitado el servicio.
# Description: Descripción detallada del servicio.
### END INIT INFO
```

El siguiente ejemplo muestra la información del archivo de inicio del servicio **sshd**:

```
#!/bin/sh
#
# sshd          Start up the OpenSSH server daemon.
#
# chkconfig: 2345 55 25
# description: SSH is a protocol for secure remote shell access.
#              This service starts up the OpenSSH server daemon.

### BEGIN INIT INFO
# Provides: sshd
# Required-Start: $local_fs $network $syslog
# Required-Stop: $local_fs $syslog
# Should-Start: $syslog
# Should-Stop: $network $syslog
# Default-Start:  2 3 4 5
# Default-Stop:  0 1 6
# Short-Description: Start up the OpenSSH server daemon
# Description:       SSH is a protocol for secure remote shell access.
#                    This service starts up the OpenSSH server daemon.
### END INIT INFO
```

Lo anterior establece que el servicio estará activo en los niveles de ejecución 2, 3, 4 y 5, el número de prioridad de inicio es 55, lo que significa que el servicio iniciará después de cualquier otro servicio con un número menor y que el número de prioridad de terminación es 25, lo que significa que el servicio será detenido antes que cualquier otro servicio con un número mayor.

8.3. Activar, desactivar, iniciar, detener o reiniciar servicios.

8.3.1. En CentOS, Fedora™ y Red Hat™ Enterprise Linux

En estos sistemas operativos, la gestión de servicios se hace a través de dos herramientas, el mandato **chkconfig** y el mandato **service**. Ambas utilizan como argumentos los nombres de los archivos de inicio de los servicios, los cuales se localizan dentro del directorio **/etc/init.d**. Ambos mandatos también están presentes en openSUSE y SUSE Enterprise Linux.

Excepto por los servicios básicos para el funcionamiento del sistema, la mayoría de los servicios están desactivados y detenidos en todos los niveles de ejecución.

8.3.1.1. Mandato chkconfig.

Para eliminar un servicio del sistema, es decir eliminar los enlaces simbólicos dentro de los sub-directorios del directorio **/etc/rc.d**, de acuerdo a la información definida en el archivo correspondiente dentro del directorio **/etc/init.d/**, se utiliza el mandato **chkconfig** con la opción **--del**. En el siguiente ejemplo se elimina el servicio sshd:

```
chkconfig --del sshd
```

Para añadir un nuevo servicio al sistema, es decir crear los enlaces simbólicos de acuerdo a la información definida en el archivo correspondiente dentro del directorio **/etc/init.d/**, se utiliza el mandato **chkconfig** con la opción **--add**. En el siguiente ejemplo se añade el servicio **sshd**:

```
chkconfig --add sshd
```

Por lo general, el mandato anterior se ejecuta automáticamente junto con la instalación de los paquetes RPM correspondientes para cada servicio. Sólo es necesario ejecutarlo cuando se instalan servicios que fueron compilados a partir de paquetes de código fuente o bien casos donde las instrucciones de instalación explícitamente solicitan hacerlo.

Para activar un servicio que ha sido previamente añadido al sistema, se ejecuta el mandato **chkconfig** con el nombre del servicio y **on** como argumentos. En el siguiente ejemplo se activa el servicio **atd**:

```
chkconfig atd on
```

Para desactivar un servicio se ejecuta el mandato **chkconfig** con el nombre del servicio y **off** como argumentos. En el siguiente ejemplo se desactiva el servicio **atd**:

```
chkconfig atd off
```

Para verificar en qué niveles de ejecución están activos o inactivos todos los servicios del sistema, se ejecuta el mandato **chkconfig** con la opción **--list**:

```
chkconfig --list
```

Para verificar en qué niveles de ejecución está activo un servicio en particular, se ejecuta el mandato **chkconfig** con la opción **--list** y el nombre del servicio a consultar. En el siguiente ejemplo se consulta en qué niveles de ejecución está activo el servicio **cups**:

```
chkconfig --list cups
```

Para activar un servicio en uno o más niveles de ejecución en particular, se ejecuta el mandato **chkconfig** con la opción **--level**, el nivel o los niveles de ejecución donde estará activo el servicio, el nombre del servicio y la cadena **on**. En el siguiente ejemplo se activa el servicio **vsftpd** sólo en los niveles de ejecución **3 y 5**:

```
chkconfig --level 35 vsftpd on
```

Para desactivar un servicio en uno o más niveles de ejecución en particular, se ejecuta el mandato **chkconfig** con la opción **--level**, el o los niveles de ejecución donde estará inactivo el servicio, el nombre del servicio y la cadena **off**. En el siguiente ejemplo se desactiva el servicio **cups** sólo en los niveles de ejecución 2 y 4:

```
chkconfig --level 24 cups off
```

Para regresar los servicios a sus valores predeterminados, se utiliza el mandato **chkconfig** con el nombre del servicio y **reset** como argumentos. En el siguiente ejemplo, se regresa a sus valores originales correspondientes al servicio **cups**:

```
chkconfig cups reset
```

Si las prioridades de inicio o terminación de servicios fueron modificados —es decir, se cambio el número de los nombres de los enlaces simbólicos de **/etc/rc.d/rc*.d**—, se ejecuta el mandato **chkconfig** con el nombre del servicio y **resetpriorities** como argumentos. En el siguiente ejemplo, se regresa a los valores originales de sus prioridades al servicio **cups**:

```
chkconfig cups resetpriorities
```

Si se quiere utilizar una herramienta muy sencilla y que es específica de CentOS, Fedora™ y Red Hat™ Enterprise Linux, puede utilizar **ntsysv**, programa que permite añadir o eliminar servicios del nivel de ejecución actual con una interfaz para modo terminal.

Herramienta ntsysv.

Si se necesita cambiar los servicios de un nivel de ejecución en particular o varios niveles simultáneos, se puede ejecutar el mandato **ntsysv** con la opción **--level** y especificando el nivel o niveles de ejecución deseados. En el siguiente ejemplo se ejecuta el mandato **ntsysv** con la opción **--level** y **3** como argumento para poder cambiar específicamente los servicios del nivel de ejecución 3:

```
ntsysv --level 3
```

En el siguiente ejemplo se ejecuta el mandato **ntsysv** con la opción **--level** y 235 como argumento para poder cambiar específicamente los servicios de los niveles de ejecución **2, 3 y 5**:

```
ntsysv --level 235
```

8.3.1.2. Mandato service.

Para iniciar cualquier servicio, se ejecuta el mandato **service** con el nombre del servicio y **start** como argumentos. En el siguiente ejemplo se inicia el servicio **atd**:

```
service atd start
```

Lo anterior equivale a ejecutar:

```
/etc/init.d/atd start
```

Para detener cualquier servicio, se ejecuta el mandato **service** con el nombre del servicio y **stop** como argumentos. En el siguiente ejemplo se detiene el servicio **atd**:

```
service atd stop
```

Lo anterior equivale a ejecutar:

```
/etc/init.d/atd stop
```

Para reiniciar cualquier servicio, se ejecuta el mandato **service** con el nombre del servicio y **restart** como argumentos. En el siguiente ejemplo se reinicia el servicio **atd**:

```
service atd restart
```

Lo anterior equivale a ejecutar:

```
/etc/init.d/atd restart
```

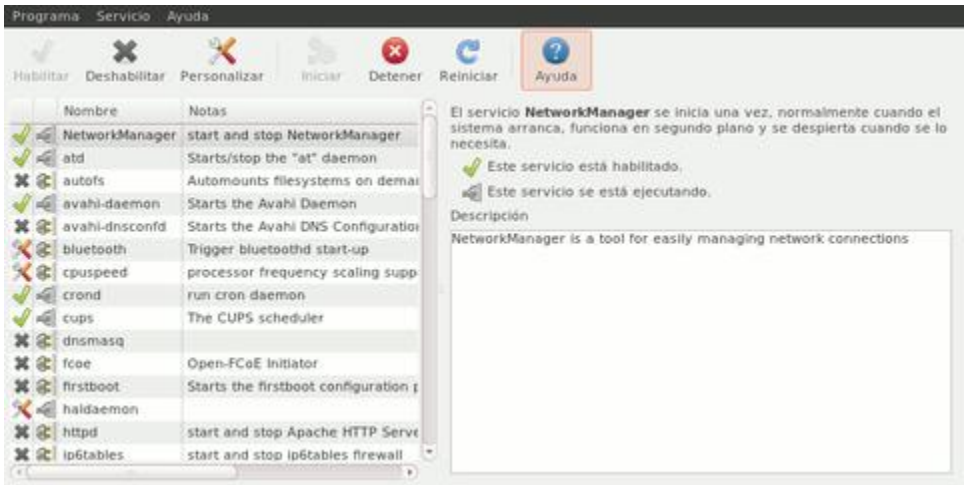
Para verificar el estado de cualquier servicio, se ejecuta el mandato **service** con el nombre del servicio y **status** como argumentos. En el siguiente ejemplo verifica el estado del servicio **atd**:

```
service atd status
```

Lo anterior equivale a ejecutar:

```
/etc/init.d/atd status
```

La herramienta **system-config-services** funciona como frente gráfico para los mandatos **chkconfig** y **service**.



Herramienta system-config-services.

8.3.2. En openSUSE™ y SUSE™ Linux Enterprise

En estos sistemas operativos, la gestión de servicios se puede realizar igualmente a través del mandato **chkconfig** y el mandato **service**, pero se prefiere utilizar el mandato **insserv** y los mandatos **rc[X]** que se instalan con cada servicio.

8.3.2.1. Mandato insserv.

Para activar un servicio se ejecuta el mandato **insserv** con el nombre del servicio como argumento. En el siguiente ejemplo se activa el servicio **sshd**:

```
insserv sshd
```

Lo anterior equivale a ejecutar:

```
chkconfig sshd on
```

Para desactivar un servicio se ejecuta el mandato **insserv** con la opción **-r** y el nombre del servicio como argumento. En el siguiente ejemplo se desactiva el servicio **sshd**:

```
insserv -r sshd
```

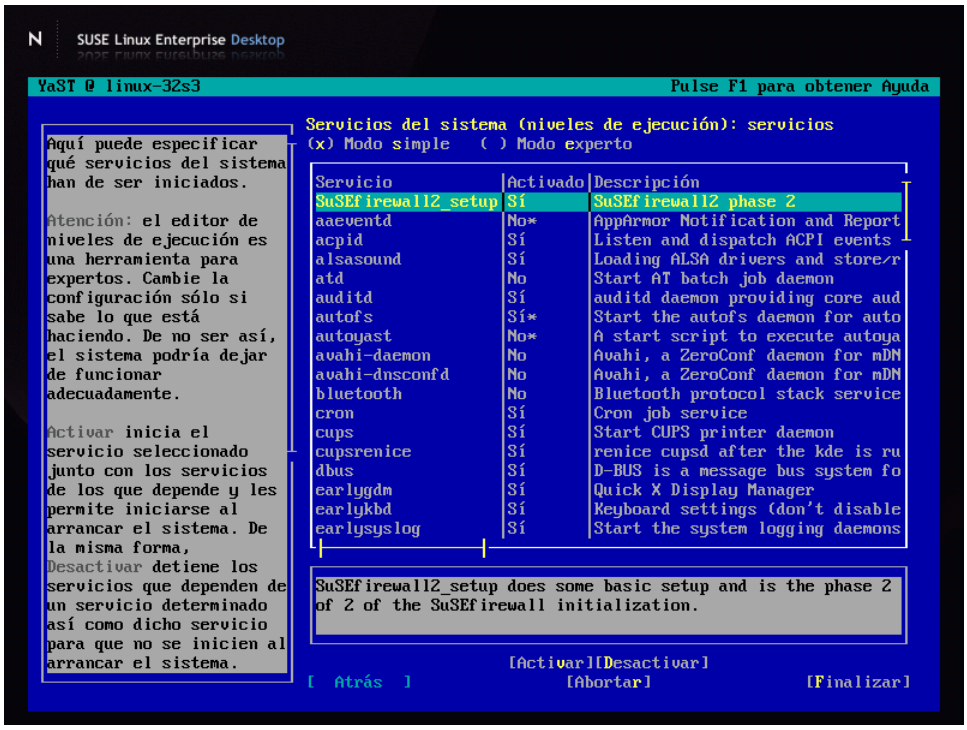
Lo anterior equivale a ejecutar:

```
chkconfig sshd off
```

El mandato **chkconfig** funciona en openSUSE™ y SUSE™ Linux Enterprise del mismo modo que en CentOS, Fedora™ o Red Hat™ Enterprise Linux y puede ser utilizado en lugar del mandato **insserv**.

Todos los procedimientos realizados por el mandato **insserv** pueden ser gestionados también a través del módulo **runlevel** de **YaST**, en modo simple, ejecutando lo siguiente:

```
yast runlevel
```



Módulo **runlevel** de **YaST**, en modo simple.

8.3.2.2. Mandatos para iniciar, detener o reiniciar servicios.

Para iniciar un servicio en particular, los paquetes en openSUSE™ y SUSE™ Linux Enterprise instalan archivos con el nombre del servicio, antecedidos por la cadena *rc*. Por ejemplo, el paquete responsable del servicio **cups** instala un enlace simbólico denominado **/usr/sbin/rccups** que apunta hacia el archivo **/etc/init.d/cups**; el paquete responsable del servicio **sshd** instala un enlace simbólico denominado **/usr/sbin/rcsshd** que apunta hacia el archivo **/etc/init.d/sshd**, etc. Todos estos mandatos son siempre enlaces simbólicos que apuntan hacia los archivos de inicio de los servicios que están en el directorio **/etc/init.d**, por lo que funcionan de modo similar a como se hace con el mandato **service** y son el método preferido en openSUSE y SUSE Enterprise Linux para iniciar, detener o reiniciar los servicios.

Para iniciar un servicio se ejecuta el mandato **rc[X]** correspondiente con **start** como argumento. En el siguiente ejemplo se inicia el servicio **sshd**:

```
rcsshd start
```

Lo anterior equivale a ejecutar:

```
/etc/init.d/sshd start
```

O bien a ejecutar:

```
service sshd start
```

Para detener un servicio se ejecuta el mandato **rc[X]** correspondiente con **stop** como argumento. En el siguiente ejemplo se detiene el servicio **sshd**:

```
rcsshd stop
```

Lo anterior equivale a ejecutar:

```
/etc/init.d/sshd stop
```

O bien a ejecutar:

```
service sshd stop
```

Para reiniciar un servicio se ejecuta el mandato **rc[X]** correspondiente con **restart** como argumento. En el siguiente ejemplo se reinicia el servicio **sshd**:

```
rcsshd restart
```

Lo anterior equivale a ejecutar:

```
/etc/init.d/sshd restart
```

O bien a ejecutar:

```
service sshd restart
```

Para verificar el estado de un servicio se ejecuta el mandato **rc[X]** correspondiente con **status** como argumento. En el siguiente ejemplo se verifica el estado del servicio **sshd**:

```
rcsshd status
```

Lo anterior equivale a ejecutar:

```
/etc/init.d/sshd status
```

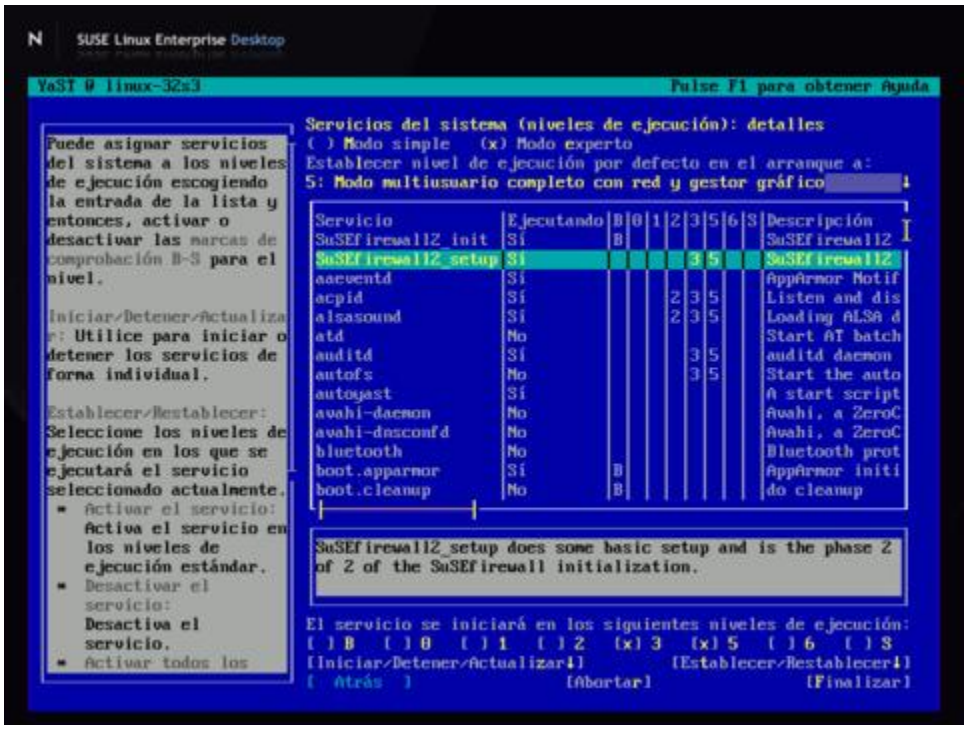
O bien a ejecutar:

```
service sshd status
```

Se puede gestionar con el módulo **runlevel** de **YaST**, en modo experto, todo lo que se realice con el mandato **insserv** y los mandatos **rc[X]**, ejecutando lo siguiente:

```
yast runlevel
```

Y luego cambiando al del modo simple al modo experto, seleccionado la casilla correspondiente.



Módulo **runlevel** de **YaST**, en modo experto.

9. Gestión de espacio de memoria de intercambio (swap) en GNU/Linux.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales **(incluyendo su publicación, a través de cualquier medio, por entidades con fines de lucro)**. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en castellano. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

9.1. Introducción.

9.1.1. Algo de historia.

Hace muchos años, **GNU/Linux**, en los tiempos del núcleo versión 2.0, se encontraba limitado a utilizar una sola partición de memoria de intercambio de un máximo de 128 MB, siendo esto una de los principales argumentos utilizados por sus detractores. Por fortuna las cosas han cambiado y hoy en día ya no existe dicho límite y es posible además utilizar cuanta memoria de intercambio sea requerida para satisfacer las necesidades de cualquier sistema.

9.1.2. ¿Qué es y como funciona el espacio de intercambio?

El espacio de memoria de intercambio o **Swap**, es lo que se conoce como **memoria virtual**. La diferencia entre la memoria real y la virtual es que está última utiliza espacio en el disco duro en lugar de un módulo de memoria. Cuando la memoria real se agota, el sistema copia parte del contenido de esta directamente en este espacio de memoria de intercambio a fin de poder realizar otras tareas.

Utilizar memoria virtual tiene como ventaja el proporcionar la memoria adicional necesaria cuando la memoria real se ha agotado y se tiene que realizar un proceso. El inconveniente radica en que, como consecuencia de utilizar espacio en el disco duro, la utilización de esta es mucho muy lenta. Uno puede percatarse de esto cuando el disco duro empieza a trabajar repentinamente hasta por varios minutos después de abrir varias aplicaciones.

¿Cuanto espacio para memoria de intercambio se debe asignar al sistema?

Menos de 1 GB RAM	Doble de la cantidad total de memoria RAM.
Más de 1 GB RAM	Misma cantidad del total de memoria RAM, más 2 GB.

9.1.3. Circunstancias en lasque se requiere aumentar la cantidad de memoria de intercambio.

Contar con mayor espacio para utilizar memoria virtual puede ser práctico en los siguientes casos:

- Sistemas en donde adquirir memoria adicional es imposible y **se está consciente que la memoria de intercambio es muchísimo más lenta** que la memoria RAM.
- En equipos con trabajo intensivo que consume mucha memoria (diseño gráfico, por ejemplo).

- Servidores de alto desempeño en donde se desea contar con un amplio margen de espacio de intercambio para satisfacer las demandas de servicios.
- Sistemas que actualizaron desde una versión de núcleo 2.2, a una versión de núcleo 2.4 o 2.6.
- Sistemas donde se aumentó la cantidad de memoria RAM y se encuentran con la problemática de cubrir la cuota mínima de espacio de memoria de intercambio.

Procedimientos.

Todos los procedimientos listados a continuación requieren hacerse como el usuario **root** o bien utilizando el mandato **sudo**.

9.1.4. Cambiar el tamaño de la partición.

Cambiar el tamaño de las particiones el disco duro y cambiar las dimensiones una partición de memoria de intercambio adicional es el método más efectivo.Sin embargo,ésto representa un riesgo, debido que podría ocurrir un error durante el procesos de repartición que podría desencadenar en pérdida de datos en un disco duro. Si se utiliza este método, es importante disponer de un respaldo de todos los datos importantes antes de comenzar el proceso.

9.1.5. Crear un archivo para memoria de intercambio.

Otro método más sencillo y sin riesgo alguno, consiste en utilizar un archivo de intercambio de forma similar a como se hace en otros sistemas operativos.

Ante todo, la mejor solución siempre será adquirir más RAM.

9.2. Procedimientos.

9.2.1. Activar una partición de intercambio adicional.

Si se cambio la tabla de particiones del disco duro y se ha creado una nueva partición de memoria de intercambio, se le da formato de la siguiente forma con el mandato **mkswap**, donde la opción **-c** indica se verifiquen sectores del disco duro buscando bloques dañados a fin de marcar estos y evitar utilizarlos:

```
mkswap -c [dispositivo]
```

En el siguiente ejemplo se dará formato como partición de memoria de intercambio a la partición **/dev/sda8**, de aproximadamente 1 GB, verificando sectores en busca de bloques dañados:

```
mkswap -c /dev/sda8
```

Lo anterior puede devolver una salida similar a la siguiente:

```
Setting up swapspace version 1, size=1048576 bytes
no label, UUID=d2fea5ab-c677-8047-789a-e54ae19c506b
```

Para activar la partición y que sea utilizada inmediatamente por el sistema operativo, se ejecuta el mandato **swapon** de la siguiente forma:

```
swapon [dispositivo]
```

En el siguiente ejemplo se activa como partición de memoria de intercambio a la partición **/dev/sda8**:

```
swapon /dev/sda8
```

Para corroborar que la nueva partición de memoria de intercambio está siendo utilizada por el sistema operativo, se ejecuta el el mandato **free**, que puede devolver una salida similar a la siguiente:

```
             total       used       free     shared    buffers     cached
Mem:        321364     312576       8788          0        940      63428
-/+ buffers/cache:     248208      73156
Swap:      1426416          0    1426416
```

Para que esta partición se utilice como memoria de intercambio automáticamente en el siguiente arranque del sistema, se edita el archivo **/etc/fstab**:

```
vim /etc/fstab
```

La línea que se deba agregar, lleva el siguiente formato:

```
[partición]             swap    swap    defaults        0 0
```

De tal modo, en el siguiente ejemplo se definirá como partición de memoria de intercambio a la partición **/dev/sda8**:

```
/dev/sda8               swap    swap    defaults        0 0
```

9.2.2. Utilizar un archivo como memoria de intercambio.

Este método no requiere hacer cambios en la tabla de particiones del disco duro. Es idóneo para usuarios poco experimentados, para quienes desean evitar tomar riesgos al cambiar la tabla de particiones el disco duro o bien para quienes requieren más de memoria de intercambio ocasional o de manera circunstancial.

Considerando que el archivo de memoria de intercambio puede ser colocado en cualquier directorio del disco duro, se ejecuta el mandato **dd**, especificando que se escribirán ceros (**if=/dev/zero**) para crear el archivo **/swap** (**of=/swap**), en bloques de 1024 bytes (**bs=1024**) hasta completar una cantidad en bytes determinada (**count=[cantidad multiplicada por el valor de bs]**). En el siguiente ejemplo se realiza lo anterior hasta completar **524288000 bytes** (**1024** por), que equivalen a **512 MB**:

```
dd if=/dev/zero of=/swap bs=1024 count=512000
```

Para dar formato de memoria de intercambio al archivo creado, se ejecuta el mandato **mkswap**, del siguiente modo:

```
mkswap /swap
```

Lo anterior puede devolver una salida similar a la siguiente:

```
Setting up swapspace version 1, size = 511996 KiB
no label, UUID=fed2aba5-77c6-4780-9a78-4ae5e19c506b
```

Para activar la partición y que sea utilizada inmediatamente por el sistema operativo, se ejecuta el mandato **swapon**. En el siguiente ejemplo se activa como partición de memoria de intercambio a el archivo **/swap**:

```
swapon /swap
```

Para corroborar que nuevo archivo de memoria de intercambio está siendo utilizada por el sistema operativo, se ejecuta el el mandato **free**, que puede devolver una salida similar a la siguiente:

```
             total       used       free     shared    buffers     cached
Mem:        321364     312576       8788          0        940      63428
-/+ buffers/cache:     248208      73156
Swap:      3145724          0    3145724
```

Para que este archivo se utilice como memoria de intercambio automáticamente en el siguiente arranque del sistema, se edita el **/etc/fstab**:

Y se agrega la línea correspondiente, del siguiente modo, donde en lugar de el dispositivo, se pone la ruta del archivo de memoria de intercambio creado:

```
vim /etc/fstab
/swap           swap    swap    defaults        0 0
```

9.2.3. Optimizando el sistema, cambiando el valor de /proc/sys/vm/swappiness

El núcleo de **GNU/Linux** permite cambiar con que frecuencia las aplicaciones y programas son movidas de la memoria física hacia la memoria de intercambio. El valor predeterminado es 60, como puede observarse al mirar el contenido de **/proc/sys/vm/swappiness** de la siguiente forma:

```
cat /proc/sys/vm/swappiness
```

Pueden establecerse valores entre 0 y 100, donde el valor más bajo establece que se utilice menos la memoria de intercambio, lo cual significa que se reclamará en su lugar el caché de la memoria. El valor predeterminado de 60, fue establecido teniendo en mente a quienes desarrollan el núcleo de Linux, con la finalidad de permitir realizar pruebas y diagnósticos.

Para la mayoría de los casos, conviene cambiar este valor por uno más bajo a fin de que el sistema utilice menos la memoria de intercambio y utilice más la **memoria cache**. Ésta es una clase de memoria RAM estática de acceso aleatorio (**SRAM** o **S**tatic **R**andom **A**ccess **M**emory). Se sitúa entre la **Unidad Central de Procesamiento** (**CPU**) y la memoria RAM y se presenta de forma temporal y automática para el usuario proporcionado acceso rápido a los datos de uso más frecuente.

Un valor apropiado y que funcionará para la mayoría de los sistemas en producción es **10**. En el siguiente ejemplo se aplica el valor **10** para el archivo **/proc/sys/vm/swappiness**.

```
echo 10 > /proc/sys/vm/swappiness
```

Para lo anterior, también se puede ejecutar el mandato **sysctl** de la siguiente forma:

```
sysctl -w vm.swappiness=10
```

Lo anterior devuelve una salida similar a la siguiente, confirmando que se ha aplicado el cambio:

```
vm.swappiness = 10
```

Este cambio en las variables del sistema de forma aplica inmediata hasta el siguiente reinicio del sistema. Para hacer que el cambio sea permanente, se edita el archivo **/etc/sysctl.conf**.

```
vim /etc/sysctl.conf
```

Y se añade la siguiente línea:

```
vm.swappiness = 10
```

10. Procedimientos de emergencia

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales **(incluyendo su publicación, a través de cualquier medio, por entidades con fines de lucro)**. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en castellano. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

10.1. Introducción.

En ocasiones suele ser necesario realizar tareas de mantenimiento y de reparación en el sistema de archivos. Estas situaciones requieren que el administrador conozca al menos las herramientas correspondientes.

10.2. Disco de rescate

El disco de instalación de CentOS y Red Hat™ Enterprise Linux incluye la opción de iniciar el sistema en modo de rescate desde éste. Seleccione la entra correspondiente o añada rescue a los argumentos de inicio.

Después de iniciar, configurar el teclado y, de forma opcional, la conectividad a través de dispositivos de red, se ingresará a un interprete de mandatos (BASH) con un conjunto básico de herramientas que permitirán realizar tareas de mantenimiento y reparación.

Digite lo siguiente a fin de mostrar en pantalla las particiones del sistema:

```
df -h
```

Lo anterior deberá mostrar algo parecido a lo siguiente:

```
S.archivos          Tamaño Usado  Disp Uso% Montado en
/dev/sda2              15G  4.8G  9.2G  34% /
/dev/sda1              76M  8.1M   64M  12% /boot
none                  507M     0  507M   0% /dev/shm
/dev/hda5              40G   35G  2.6G  94% /home
/dev/sdb3             2.0G   36M  1.9G   2% /tmp
/dev/sdb1             6.4G  4.0G  2.2G  66% /usr/local
/dev/sdb5             6.4G  4.3G  1.8G  71% /usr/src
/dev/sdb2             2.0G  570M  1.4G  30% /var
/dev/hda6              19G   17G  998M  95% /var/ftp
/dev/hda2             6.0G  257M  5.4G   5% /var/lib
/dev/hda1             6.9G  792M  5.8G  12% /var/www
```

10.3. Verificación de la integridad del disco

La verificación de cualquier partición del disco duro requiere, necesariamente, desmontar antes ésta. Utilizar el mandato **fsck** en una partición montada, puede ocasionar la pérdida o corrupción de datos. Una vez desmontada la partición a verificar, es posible realizar una verificación y/o reparación utilizando cualquiera de los siguientes ejemplos de uso del mandato **fsck**.

Forzar la verificación del sistema de archivos, responder automáticamente con *«Si»* (opción **-y**) a la reparación de cualquier problema que requiera intervención humana (opción **-y**) y mostrando una barra de progreso (opción **-C**).

```
fsck -fyC /dev/sdXX
```

Forzar la verificación del sistema de archivos y responder automáticamente con *«Si»* (opción **-y**) a la reparación de cualquier problema que requiera intervención humana (opción **-y**).

```
fsck -fy /dev/sdXX
```

Lo mismo que el mandato anterior, pero además con verificación de solo-lectura para buscar bloques dañados (opción **-c**), preservando la lista de bloques dañados existente donde se añadirán nuevos bloques dañados a ésta (opción **-k**).

```
fsck -fykc /dev/sdXX
```

Lo mismo que el mandato anterior, pero con verificación de **lectura-escritura no-destructiva** para buscar bloques dañados (opción **-cc**), preservando la lista de bloques dañados existente donde se añadirán nuevos bloques dañados a ésta (opción **-k**). Sí se encuentra un bloque dañado, este se añade al inodo de bloques dañados.

```
fsck -fykcc /dev/sdXX
```

Forzar la verificación del sistema de archivos, reparar automáticamente cualquier problema que pueda ser resuelto **sin** intervención humana (opción **-p**) y mostrando una barra de progreso (opción **-C**).

```
fsck -fpC /dev/sdXX
```

Forzar la verificación del sistema de archivos y reparar automáticamente cualquier problema que pueda ser resuelto **sin** intervención humana (opción **-p**).

```
fsck -fp /dev/sdXX
```

Lo mismo que el mandato anterior, pero además con verificación de solo-lectura para buscar bloques dañados (opción **-c**), preservando la lista de bloques dañados existente donde se añadirán nuevos bloques dañados a ésta (opción **-k**).

```
fsck -fpkc /dev/sdXX
```

Lo mismo que el mandato anterior, pero con verificación de **lectura-escritura no-destructiva** para buscar bloques dañados (opción **-cc**), preservando la lista de bloques dañados existente donde se añadirán nuevos bloques dañados a ésta (opción **-k**). Sí se encuentra un bloque dañado, este se añade al inodo de bloques dañados.

```
fsck -fpkcc /dev/sdXX
```

Verificar el sistema de archivos, reparando automáticamente cualquier problema que pueda ser resuelto sin intervención humana y tratando de optimizar los directorios del sistema de archivos (opción **-D**).

```
fsck -fpD /dev/sdXX
```

La optimización de directorios se realiza volviendo a crear un índice de éstos sí el sistema de archivos incluye soporte para índices (como es el caso de Ext4) o bien re-ordenando y comprimiendo directorios en los casos de directorios pequeños o bien sistemas de archivos que utilicen directorios lineales tradicionales.

Lo mismo que el mandato anterior, pero con verificación de lectura-escritura no-destructiva para buscar bloques dañados (opción **-cc**), preservando la lista de bloques dañados existente donde se añadirán nuevos bloques dañados a ésta (opción **-k**). Sí se encuentra un bloque dañado, este se añade al *inodo* (nodo índice) de bloques dañados.

```
fsck -fpDkcc /dev/sdXX
```

10.4. Respaldo y restauración del sector de arranque maestro.

Los primeros 512 bytes del disco duro o unidad de almacenamiento utilizado para el sistema operativo, corresponde al sector de arranque maestro, donde:

- Los primeros 446 bytes corresponden al gestor de arranque
- Los siguientes 64 bytes corresponden a la tabla de particiones. 16 bytes para cada partición primaria y/o extendida que existan.
- Los últimos 2 bytes corresponden a la firma de unidad arrancable. También se les conoce como los 2 bytes mágicos.

Para realizar un respaldo del sector de arranque maestro, se puede utilizar el mandato dd del siguiente modo:

```
dd if=/dev/sda of=mbr.bin bs=512 count=1
```

Para restaurar el sector de arranque maestro, se utiliza el mandato dd del siguiente modo:

```
dd if=mbr.bin of=/dev/sda bs=512 count=1
```

Para respaldar exclusivamente el gestor de arranque, se utiliza el mandato dd del siguiente modo:

```
dd if=/dev/sda of=gestor.bin bs=446 count=1
```

Para restaurar el gestor de arranque, se utiliza el mandato dd del siguiente modo:

```
dd if=gestor.bin of=/dev/sda bs=446 count=1
```

Para respaldar exclusivamente la tabla de particiones, se utiliza el mandato dd del siguiente modo:

```
dd if=/dev/sda of=tabla.bin skip=446 bs=1 count=64
```

Para restaurar exclusivamente la tabla de particiones, se utiliza el mandato dd del siguiente modo:

```
dd if=tabla.bin of=/dev/sda seek=446 bs=1 count=64
```

Para borrar exclusivamente el gestor de arranque, utilice el mandato dd del siguiente modo:

```
dd if=/dev/zero of=/dev/sda bs=446 count=1
```

Para borrar exclusivamente la tabla de particiones, algo que nadie en su sano juicio haría sin tener un respaldo a la mano, utilice el mandado dd del siguiente modo:

```
dd if=/dev/zero of=/dev/sda seek=446 bs=1 count=64
```

Para borrar todo el sector de arranque completo, es decir el gestor de arranque, tabla de particiones y los dos bytes mágicos, utilice el mandato dd del siguiente modo

```
dd if=tabla.bin of=/dev/sda bs=512 count=1
```

Tenga cuidado al ejecutar cualquiera de los mandatos anteriores, pues si se equivoca se corre el riesgo de dañar de manera irreversible los datos del disco duro o unidad de almacenamiento utilizada.

10.5. Asignación de formato de las particiones

Cuando la situación lo amerite, será posible dar formato a una partición en particular con formato EXT3 de la siguiente forma:

```
mkfs.ext3 /dev/sda1
```

Cuando la situación lo amerite, será posible dar formato a una partición en particular con formato EXT4 de la siguiente forma:

```
mkfs.ext4 /dev/sda1
```

Se encuentran también disponibles las siguientes herramientas para asignación de formato:

- mkfs.ext2
- mkfs.vfat (fat32)
- mkfs.msdos (fat16)
- mkswap

Si se necesita dar un formato de bajo nivel a fin de eliminar toda la información del disco duro, puede utilizarse lo siguiente, considerando en el ejemplo que se intenta dar formato de bajo nivel al disco duro **/dev/sda**, para escribir 0 (ceros) en cada sector del disco duro.

```
dd if=/dev/zero of=/dev/sda
```

Si se requiere, también es posible dar formato de bajo nivel escribiendo números aleatorios en todos los sectores del disco duro:

```
dd if=/dev/urandom of=/dev/sda
```

11. Gestión de volúmenes lógicos.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales (incluyendo su publicación, a través de cualquier medio, por entidades con fines de lucro). c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en castellano. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

11.1. Introducción.

LVM es una implementación que consiste en un administrador de volúmenes lógicos para el núcleo de Linux. Fue originalmente escrito en 1998 por Heinz Mauelshagen, quien se basó sobre el administrador de volúmenes de Veritas, el cual solía ser utilizado en en sistemas HP-UX.

Básicamente, LVM2 permite hacer lo siguiente:

- Cambio de tamaño de grupos de volúmenes.
- Cambio de tamaño de volúmenes lógicos.
- Instantáneas de lectura y escritura (a partir de LVM2).
- RAID0 de volúmenes lógicos.

LVM carece de soporte para implementar RAID1 o RAID5, por lo que se recomienda configurar este tipo de arreglos RAID, trabajando con volúmenes lógicos por encima de los arreglos RAID.

LVM se compone de tres partes:

1. Volúmenes físicos (pv, physical volume). Son particiones en el disco duro, con la bandera 8e. Se pueden dividir en extensiones físicas (pe o physical extents).
2. Volúmenes lógico (lv o logical volume). Se componen de volúmenes físicos. Se pueden dividir en extensiones lógicas (le, logical extents).
3. Grupos de volúmenes (vg o volume group). Se componen de uno o más volúmenes lógicos utilizados y volúmenes físicos sin utilizar. Son unidades administrativas donde se agrupan los recursos.

Procedimientos.

11.1.1. Crear un volumen lógico a partir de un disco duro nuevo.

Ejecute el mandato **parted** para crear una nueva etiqueta en el disco duro nuevo.

```
parted /dev/sdb mklabel msdos
```

Utilice nuevamente el mandato **parted** para crear una partición primaria tipo ext4, que tendrá 10240 GB (inicio en 1, fin en 10240):

```
parted /dev/sdb mkpart primary ext4 1 10480
```

Cambie el tipo de partición a LVM:

```
parted /dev/sdb set 1 lvm on
```

Para visualizar la tabla de particiones y verificar que se ha creado una partición primaria de 10240 MB, tipo LVM, ejecute lo siguiente:

```
parted /dev/sdb print
```

Lo anterior debe devolver una salida similar al al siguiente:

```
Model: ATA VBOX HARDDISK (scsi)
Disk /dev/sdb: 21.5GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos

Numero  Inicio  Fin     Tamaño  Typo     Sistema de ficheros  Banderas
 1      1049kB  10.5GB  10.5GB  primary                       lvm
```

Para presentar la nueva partición ante el núcleo del sistema, ejecute el mandato **partprobe** del siguiente modo:

```
partprobe /dev/sdb1
```

Nota.

Si lo anterior falla, ejecute el mandato **hdaparm** del siguiente modo:

```
hdparm -z /dev/sdb
```

Para crear un volumen físico, ejecute el mandato **pvcreate** del siguiente modo:

```
pvcreate /dev/sdb1
```

Ejecute el mandato **pvscan** para verificar el procedimiento anterior:

```
pvscan
```

Lo anterior deberá devolver una salida similar a la siguiente:

```
  PV /dev/sda2   VG VolGroup00 lvm2 [53.80 GiB / 0    free]
  PV /dev/sda3   VG VolGroup01 lvm2 [8.00 GiB / 0    free]
  PV /dev/sdb1                  lvm2 [9.76 GiB]
  Total: 3 [71.55 GiB] / in use: 2 [61.79 GiB] / in no VG: 1 [9.76 GiB]
```

Para crear el grupo de volúmenes denominado VolDatos, ejecute el mandato **vgcreate** del siguiente modo:

```
vgcreate VolDatos00 /dev/sdb1
```

Ejecute el mandato **vgscan** para verificar el procedimiento anterior:

```
vgscan
```

Lo anterior deberá devolver una salida similar a la siguiente:

```
  Reading all physical volumes.  This may take a while...
  Found volume group "VolDatos00" using metadata type lvm2
  Found volume group "VolGroup00" using metadata type lvm2
  Found volume group "VolGroup01" using metadata type lvm2
```

Para crear un volumen lógico, denominado Datos00, perteneciente al grupo de volúmenes denominado VolDatos, asignando el 100% de las extensiones lógicas libres, ejecute el mandato **lvcreate** del siguiente modo:

```
lvcreate -l 100%FREE VolDatos00 -n Datos00
```

Ejecute el mandato **lvscan** para verificar el procedimiento anterior:

```
lvscan
```

Lo anterior deberá devolver una salida similar a la siguiente:

```
  ACTIVE            '/dev/VolDatos00/Datos00' [9.76 GiB] inherit
  ACTIVE            '/dev/LogVol00/LogVol01' [53.80 GiB] inherit
  ACTIVE            '/dev/LogVol01/LogVol00' [8.00 GiB] inherit
```

Para dar formato al nuevo volumen lógico, ejecute el mandato mkfs.ext4 del siguiente modo:

```
mkfs.ext4 /dev/VolDatos00/Datos00
```

Ejecute el mandato **mkdir** para crear el punto de montaje /datos:

```
mkdir /datos
```

Para montar el volumen lógico en el directorio /datos, ejecute lo siguiente:

```
mount /dev/VolDatos00/Datos00 /datos
```

Ejecute el mandato **df** para verificar el procedimiento anterior:

```
df
```

Lo anterior deberá devolver una salida similar a la siguiente:

```
S.ficheros         Bloques de 1K   Usado    Dispon Uso% Montado en
/dev/mapper/VolGroup00-LogVol00
                      26351440    221008  26130432   1% /
tmpfs                   319096        88    319008   1% /dev/shm
/dev/sda1               198337     24376    163721  13% /boot
/
/dev/mapper/VolDatos00-Datos00
                      10071208    153560   9406060   2% /datos
```

Para que el volumen lógico se monte automáticamente al iniciar el sistema, edite el archivo /etc/fstab:

```
vim /etc/fstab
```

Añada el siguiente contenido:

```
/dev/mapper/VolDatos00-Datos00   /datos   ext4   defaults,noatime,nodiratime   1 2
```

Desmonte y monte de nuevo el volumen lógico para verificar que todo trabaje correctamente.

```
umount /datos
mount /datos
```

11.1.1.1. Mover contenidos desde un volumen físico a otro en un nuevo disco duro.

Asumiendo que se ha realizado todo el procedimiento anterior y que el contenido actual del volumen lógico es menor al tamaño del nuevo volumen físico añadido al volumen lógico, sólo se requiere utilizar el mandato **pvmove** para mover el contenido de un volumen físico a otro.

```
pvmove /dev/sda1 /dev/sdb1
```

Una vez terminado el movimiento, asumiendo que el tamaño del volumen físico en /dev/sdb1, es igual o mayor al del volumen físico en /dev/sda1, sólo resta eliminar /dev/sda1 del volumen lógico.

```
vgreduce VolGroup00 /dev/sda1
```

11.1.2. Añadir un volumen físico a un volumen lógico existente, a partir de espacio libre sin particionar en un disco duro.

Se asume un escenario donde:

- Se utilizará el mismo disco duro del procedimiento anterior y que corresponde al dispositivo /dev/sdb
- El grupo de LVM al cual se añadirá el disco es VolGroup00
- Que el volumen lógico que se hará crecer con un nuevo volumen físicos, será LogVol00.

Determine el espacio disponible del disco duro, ejecutando el mandato **parted** del siguiente modo:

```
parted /dev/sdb unit MB print free
```

Determine en qué MB comienza el espacio libre.

Para crear una nueva partición de aproximadamente 5120 MB, ejecute el mandato **parted** del siguiente modo:

```
parted /dev/sdb mkpart primary ext4 10481 15600
```

Nota.

Es posible que el sistema devuelva una advertencia que indica que se necesita reiniciar para que el núcleo de Linux pueda leer la nueva tabla de particiones:

```
Aviso: WARNING: the kernel failed to re-read the partition table on /dev/sdb
(Dispositivo o recurso ocupado). As a result, it may not reflect all of your changes
until after reboot.
```

Ignore la advertencia y continúe trabajando. De ser necesario, reinicie el sistema más adelante o bien ejecute el mandato **partprobe** del siguiente modo:

```
partprobe /dev/sdb2
```

Si lo anterior falla, ejecute el mandato **hdaparm** del siguiente modo:

```
hdparm -z /dev/sdb
```

Cambie el tipo de partición a LVM:

```
parted /dev/sdb set 2 lvm on
```

Para visualizar la tabla de particiones y verificar que se ha creado una partición primaria de 5120 MB, tipo LVM, ejecute lo siguiente:

```
parted /dev/sdb print
```

Lo anterior deberá devolver una salida similar a la siguiente:

```
Model: ATA VBOX HARDDISK (scsi)
Disk /dev/sdb: 21.5GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos

Numero  Inicio  Fin     Tamaño  Typo     Sistema de ficheros  Banderas
 1      1049kB  10.5GB  10.5GB  primary                       lvm
 2      10.5GB  15.6GB  5119MB  primary                       lvm
```

Para crear un volumen físico, ejecute el mandato **pvcreate** del siguiente modo:

```
pvcreate /dev/sdb2
```

Ejecute el mandato **pvscan** para verificar el procedimiento anterior:

```
pvscan
```

Lo anterior deberá devolver una salida similar a la siguiente:

```
  PV /dev/sda2   VG VolGroup00 lvm2 [53.80 GiB / 0    free]
  PV /dev/sda3   VG VolGroup01 lvm2 [8.00 GiB / 0    free]
  PV /dev/sdb2                 lvm2 [4.77 GiB]
  Total: 4 [76.32 GiB] / in use: 3 [71.55 GiB] / in no VG: 1 [4.77 GiB]
```

Para añadir este volumen físico, que corresponde a la partición /dev/sdb2, al grupo de volúmenes denominado VolGroup00, ejecute el mandato vgextend del siguiente modo:

```
vgextend VolGroup00 /dev/sdb2
```

Lo anterior debe devolver una salida similar a la siguiente:

```
  Volume group "VolGroup00" successfully extended
```

Para asignar el 100% nuevo espacio libre disponible, provisto por el nuevo volumen físico añadido al grupo de volúmenes denominado VolGroup00, al volumen lógico LogVol00, ejecute el mandato lvextend del siguiente modo:

```
lvextend -l +100%FREE /dev/VolGroup00/LogVol00
```

Lo anterior debe devolver una salida similar a la siguiente:

```
  Extending logical volume LogVol00 to 31.66 GiB
  Logical volume LogVol00 successfully resized
```

Para cambia el tamaño del sistema de archivos y que éste utiliza el nuevo espacio libre recién asignado al volumen lógico, ejecute el mandato resize2fs del siguiente modo:

```
resize2fs /dev/VolGroup00/LogVol00
```

Lo anterior debe devolver una salida similar a la siguiente:

```
resize2fs 1.41.12 (17-May-2010)
Filesystem at /dev/Datos/LogVol00 is mounted on /home; on-line resizing required
old desc_blocks = 2, new_desc_blocks = 2
Performing an on-line resize of /dev/Datos/LogVol00 to 8300544 (4k) blocks.
El sistema de ficheros en /dev/VolGroup00/LogVol00 tiene ahora 8300544 bloques.
```

Ejecute df, con la opción -h, para ver el nuevo tamaño de del sistema de archivos alojado en /dev/VolGroup00/LogVol00:

```
df -h
```

Lo anterior debe devolver una salida similar a la siguiente:

```
S.ficheros            Size  Used Avail Use% Montado en
/dev/mapper/VolGroup00-LogVol00
                       32G  216M   30G   1% /
/dev/sda1             194M   24M  160M  13% /boot
/dev/mapper/VolDatos00-Datos00
                      9.7G  229M  8.9G   3% /datos
```

11.1.3. Quitar una unidad física a un volumen lógico.

Antes de proceder, es importante contar con un respaldo de los datos almacenados en el volumen lógico al cual se le quitará la unidad física. Verifique que el respaldo es confiable.

Este procedimiento requiere que el volumen lógico esté sin montar. Si se trata de un volumen lógico cuyo sistema de archivos esté en uso, como /, /usr o /var, el procedimiento debe hacerse desde un disco vivo o bien utilizando el disco de instalación en modo de rescate.

Inicie el sistema con el disco de instalación en modo de rescate.

Ejecute el mandato **df** y desmonte todas las particiones que estén debajo del directorio /mnt/sysimage.

Ejecute el mandato **fsck**, con la opción -f, para verificar la partición a reducir.

```
fsck -f /dev/VolGroup00/LogVol00
```

Para determinar el tamaño al que debe reducirse el sistema de archivos, ejecute el mandato **parted** del siguiente modo:

```
parted /dev/sdb print
```

Ejecute el mandato resize2fs para reducir el tamaño del sistema de archivos, a una cantidad

Desmonte la partición

Ejecute el mandato pvdisplay para determinar el tamaño de las particiones /dev/sda2 y /dev/sdb2 y cuantas extensiones físicas contienen cada una.

```
pvdisplay /dev/sda2 /dev/sdb2
```

Lo anterior debe devolver una salida similar a la siguiente:

```
  --- Physical volume ---
  PV Name               /dev/sda2
  VG Name               VolGroup00
  PV Size               53.80 GiB / not usable 4.00 MiB
  Allocatable           yes (but full)
  PE Size               4.00 MiB
  Total PE              13772
  Free PE               0
  Allocated PE          13772
  PV UUID               jZCHg7-ub0R-kziP-hCy6-V12S-tXRm-2qXont

  --- Physical volume ---
  PV Name               /dev/sdb2
  VG Name               VolGroup00
  PV Size               4.77 GiB / not usable 2.00 MiB
  Allocatable           yes (but full)
  PE Size               4.00 MiB
  Total PE              1220
  Free PE               0
  Allocated PE          1220
  PV UUID               lk6bMt-3vci-yw1p-Te2w-KPot-kpje-l18cAB
```

Primero hay que reducir el tamaño del sistema de archivos involucrado, de modo que el nuevo tamaño sea ligeramente menor al tamaño del volumen físico que se continuará utilizando en el volumen lógico, siempre y cuando el espacio utilizado del sistema de archivos sea menor al tamaño del volumen físico que se conservara. Si se reduce el tamaño del sistema de archivos, a uno menor al del espacio utilizado por el contenido actual, se perderán todos los datos.

Asumiendo un escenario como el del ejemplo de arriba, donde el tamaño del volumen físico que se conservará es de 53.80 GB, defina 52 GB.

```
resize2fs /dev/VolGroup00/LogVol00 52G
```

Lo anterior debe devolver una salida similar a la siguiente:

```
Resizing the filesystem on /dev/Datos/LogVol00 to 7077888 (4k) blocks.
El sistema de ficheros en /dev/Datos/LogVol00 tiene ahora 7077888 bloques.
```

Vuelva a verificar el volumen lógico con el mandato **fsck**, del siguiente modo:

```
fsck -f /dev/VolGroup00/LogVol00
```

Asumiendo un escenario donde el volumen físico que se eliminará del volumen lógico tiene 1220 extensiones, para restar del volumen lógico estas extensiones físicas, ejecute el mandato lvresize del siguiente modo:

```
lvresize -l -1220 /dev/VolGroup00/LogVol00
```

Lo anterior le mostrará una advertencia, la cual indica que tiene un alto riesgo reducir el tamaño del volumen lógico y que es posible se pierdan todos los datos. Es precisamente por ésto que se redujo primero el tamaño del sistema de archivos.

```
  WARNING: Reducing active logical volume to 26.90 GiB
  THIS MAY DESTROY YOUR DATA (filesystem etc.)
Do you really want to reduce LogVol00? [y/n]:
```

Si el tamaño del sistema de archivos es menor al tamaño que se asignará después de eliminar las extensiones, correspondientes al volumen físico que se eliminará, puede responder con una y sin temor a perder los datos contenidos en el volumen lógico.

```
  WARNING: Reducing active logical volume to 26.90 GiB
  THIS MAY DESTROY YOUR DATA (filesystem etc.)
Do you really want to reduce LogVol00? [y/n]:y
  Reducing logical volume LogVol00 to 26.90 GiB
  Logical volume LogVol00 successfully resized
```

Para eliminar el volumen físico del grupo de volúmenes denominado VolGroup00, ejecute lo siguiente:

```
vgreduce VolGroup00 /dev/sdb2
```

Lo anterior debe devolver una salida similar a la siguiente:

```
  Removed "/dev/sdb2" from volume group "Datos"
```

Como precaución, se redujo el tamaño del sistema de archivos a una cantidad menor a la disponible en el volumen físico que se conservó. Ésto deja espacio libre que probablemente se quiera utilizar. Para cambiar el tamaño del sistema de archivos y que tome todo el espacio disponible en el volumen lógico, ejecute el mandato resize2fs del siguiente modo:

```
resize2fs /dev/VolGroup00/LogVol00
```

Lo anterior debe devolver una salida similar a la siguiente:

```
resize2fs 1.41.12 (17-May-2010)
Filesystem at /dev/Datos/LogVol00 is mounted on /home; on-line resizing required
old desc_blocks = 2, new_desc_blocks = 2
Performing an on-line resize of /dev/Datos/LogVol00 to 7051264 (4k) blocks.
El sistema de ficheros en /dev/Datos/LogVol00 tiene ahora 7051264 bloques.
```

Vuelva a verificar la partición, ejecutando el mandato **fsck** del siguiente modo.

```
fdisk -f /dev/VolGroup00/LogVol00
```

Monte la partición en el directorio que le corresponda y verifique que contiene datos. Al terminar reinicie el sistema y retire el disco de rescate.

11.2. Bibliografía.

- https://secure.wikimedia.org/wikipedia/es/wiki/LVM

12. Gestión de RAID a través de MDADM.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales (incluyendo su publicación, a través de cualquier medio, por entidades con fines de lucro). c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en castellano. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

12.1. Introducción

MDADM (***M****ultiple* ***D****evice* ***Adm****inistrator*) es un conjunto de herramientas que son utilizadas en GNU/Linux para la gestión de RAID (***R****edundant* ***A****rray of* ***I****ndependent* ***D****isks*, que se traduce como conjunto redundante de discos independientes) administrado a través de software, distribuido bajo los términos de la Licencia Pública General de GNU versión 2 (GNU/GPLv2).

El RAID por software permite:

- Una solución de RAID de muy bajo costo pues prescinde del uso de costosas tarjetas RAID y unidades de almacenamiento especiales y que carece de restricciones que regularmente imponen los fabricantes de dispositivos de hardware privativos.
- Proceso de reconstrucción de arreglos en subprocesos.
- Configuración basada sobre el núcleo del sistema.
- Permite portar de manera transparente los arreglos entre sistemas GNU/Linux sin necesidad de reconstruir éstos.
- Mejor aprovechamiento de los recursos del sistema pues la reconstrucción de los arreglos se hace utilizando recursos libres.
- Soporte para unidades de almacenamiento con capacidad para realizar cambios en caliente (hot-swap).
- Detección automática del número de núcleos del microprocesador a fin de aprovechar mejor los recursos del sistema.

URL: kernel.org/pub/linux/utils/raid/mdadm/.

12.1.1. Tipos de arreglos soportados.

MDADM permite configurar los siguientes arreglos RAID:

- **RAID0**: Incrementa el índice de transmisión del sistema (*throughput*) mediante el uso de varias unidades de disco en paralelo. El rendimiento del sistema con la configuración RAID0 es superior a la que proporcionan las configuraciones RAID1 o RAID5, pero se incrementa la posibilidad de pérdida de datos porque no hay forma de recuperar o reconstruir los datos almacenados en cualquier disco que falle. Requiere 2 discos.

- **RAID1**: Espejo. El arreglo más lento de todos. Requiere 2 unidades de almacenamiento.

- **RAID4**: Igual que RAID0 pero con una unidad de almacenamiento extra para mejorar el desempeño a través de la paridad y al mismo tiempo lograr redundancia. Requiere 4 unidades de almacenamiento.

- **RAID5**: Igual a RAID4 pero con una paridad distribuida en todas la unidades de almacenamiento. Requiere un mínimo de 3 unidades de almacenamiento.

- **RAID6**: Igual que RAID5 pero con dos paridades. Requiere un mínimo de 4 unidades de almacenamiento.

- **RAID10**: Se le conoce mejor como RAID1+0. Combina RAID1 y RAID0. Requiere un mínimo de 4 unidades de almacenamiento.

Nota.

Un RAID0+1 (también llamado RAID01 y que es muy diferente a RAID1 y totalmente opuesto a RAID1+0) es un arreglo usado para replicar y compartir datos entre varios discos. Un RAID0+1 es un espejo de divisiones. Es decir, dos arreglos RAID0 en el nivel inferior y un arreglo RAID1 en el nivel superior. Una falla de disco en RAID0+1 resulta en un una falla completa de uno de los arreglos RAID0 en el nivel inferior y degradación del arreglo en RAID1 en el nivel superior.

RAID10 es lo contrario a un RAID0+1, pues los niveles RAID que lo forman se invierten: un RAID10 es una división de espejos. Es decir un RAID0 en el nivel superior y dos arreglos RAID1 en el nivel inferior. Una falla de disco sólo degrada uno de los espejos del nivel inferior sin afectar el RAID0 en el nivel superior, salvo por el desempeño que se pierde por la falta de paridad.

MDADM permite también configurar los siguientes arreglos No-RAID:

- **LINEAR**: Concatena unidades de almacenamiento en un sólo dispositivo md.

- **MULTIPATH**: permite múltiples rutas con falla en un sólo dispositivo.

- **FAULTY**: Un dispositivo que emula varios escenarios de falla de disco. Sólo se utiliza para pruebas y desarrollo.

- **CONTAINER**: Grupo de dispositivos que son gestionados como un único dispositivo sobre el cual se pueden crear dispositivos RAID.

Equipamiento lógico necesario.

El paquete mdadm viene instalado de modo predeterminado en **ALDOS**, **Fedora™**, **CentOS** y **Red Hat™ Enterprise Linux**, pues se trata de un paquete obligatorio. Si por algún motivo estuviese ausente, instale o actualice el paquete mdadm.

```
yum -y install mdadm
```

Reinicie el sistema sólo en caso de que el paquete hubiera estado ausente de la instalación, pues debe iniciar junto con el servicio **mdmonitor**.

12.2. Procedimientos.

Se asume que se han añadido varias unidades de almacenamiento en el sistema. Todas las unidades de almacenamiento que formen parte de un mismo arreglo siempre deben ser idénticas en capacidad.

Para listar las capacidades la primera unidad de almacenamiento libre y disponible (/dev/sdb) ejecute lo siguiente.

```
fdisk -l /dev/sdb
```

La salida debe ser similar a la siguiente:

```
Disco /dev/sdb: 8589 MB, 8589934592 bytes
255 heads, 63 sectors/track, 1044 cylinders
Units = cilindros of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000
```

Para listar las capacidades la siguiente unidad de almacenamiento (/dev/sdc) ejecute lo siguiente

```
fdisk -l /dev/sdc
```

La salida debe ser similar a la siguiente:

```
Disco /dev/sdc: 8589 MB, 8589934592 bytes
255 heads, 63 sectors/track, 1044 cylinders
Units = cilindros of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000
```

Compruebe que las unidades involucradas son **exactamente** de la misma capacidad.

12.2.1. Crear un arreglo tipo RAID1.

Ejecute lo siguiente para crear dispositivo RAID1, indicando el número de dispositivos que lo integrarán y las unidades de almacenamiento a utilizar.

```
mdadm --create /dev/md0 --level=1 \
    --raid-devices=2 /dev/sdc /dev/sdb
```

La salida siempre devuelve una advertencia que recuerda que se debe evitar utilizar dispositivos RAID con MDADM para /boot porque muchos gestores de arranque carecen de soporte para metadatos versión 1.x y que se recomienda usar --metadata=0.90. Pase por alto esta advertencia porque —al menos para los escenarios descritos en este documento— el arreglo sólo se utilizará para almacenar datos.

```
mdadm: Note: this array has metadata at the start and
    may not be suitable as a boot device.  If you plan to
    store '/boot' on this device please ensure that
    your boot-loader understands md/v1.x metadata, or use
    --metadata=0.90
Continue creating array?
```

Responda pulsado **y** para proceder.

Observe la información del arreglo:

```
mdadm --detail --scan
```

La salida de lo anterior puede ser similar a la siguiente.

```
ARRAY /dev/md0 metadata=1.2 name=0 UUID=ae6c23ea:c62d0933:7e89faee:1174c7d2
```

Ejecute lo siguiente para guardar la información del arreglo recién creado en el archivo **/etc/mdadm.conf**

```
mdadm --detail --scan >> /etc/mdadm.conf
```

Espere a que el arreglo se construya. Se puede ver el estado de progreso ejecutando lo siguiente:

```
mdadm --detail /dev/md0
```

Lo anterior puede devolver algo similar a lo siguiente:

```
/dev/md0:
        Version : 1.2
  Creation Time : Tue Jun 11 22:25:30 2013
     Raid Level : raid1
     Array Size : 8384448 (8.00 GiB 8.59 GB)
  Used Dev Size : 8384448 (8.00 GiB 8.59 GB)
   Raid Devices : 2
  Total Devices : 2
    Persistence : Superblock is persistent

    Update Time : Tue Jun 11 22:25:45 2013
          State : active, resyncing
 Active Devices : 2
Working Devices : 2
    Persistence : Superblock is persistent

         Layout : near=2
     Chunk Size : 512K

  Resync Status : 44% complete

           Name : 1
           UUID : 3ae6c23ea:c62d0933:7e89faee:1174c7d2
         Events : 8

    Number   Major   Minor   RaidDevice State
       0       8       32        0      active sync   /dev/sdc
       1       8       16        1      active sync   /dev/sdb
```

Mientras se va construyendo el arreglo, observe que el valor de ***State*** es ***active, resyncing***. El valor de ***Resync Status*** informará respecto del porcentaje de progreso de la operación. El proceso puede demorar desde unos pocos minutos hasta varias horas dependiendo el tamaño de las unidades de almacenamiento utilizadas.

Cuando el arreglo esté terminado el valor mostrado por ***State*** debe ser sólo **active**. Ejemplo:

```
/dev/md0:
        Version : 1.2
  Creation Time : Tue Jun 11 22:25:30 2013
     Raid Level : raid1
     Array Size : 8384448 (8.00 GiB 8.59 GB)
  Used Dev Size : 8384448 (8.00 GiB 8.59 GB)
   Raid Devices : 2
  Total Devices : 2
    Persistence : Superblock is persistent

    Update Time : Tue Jun 11 22:26:18 2013
          State : active
 Active Devices : 2
Working Devices : 2
 Failed Devices : 0
  Spare Devices : 0

           Name : 0
           UUID : ae6c23ea:c62d0933:7e89faee:1174c7d2
         Events : 18

    Number   Major   Minor   RaidDevice State
       0       8       32        0      active sync   /dev/sdc
       1       8       16        1      active sync   /dev/sdb
```

Puede verificarse un resumen del estado a través de **/proc/mdstat**.

```
cat /proc/mdstat
```

Lo anterior puede devolver una salida similar a la siguiente:

```
Personalities : [raid1]
md0 : active raid1 sdb[1] sdc[0]
      8384448 blocks super 1.2 [2/2] [UU]

unused devices: <none>
```

A partir de este momento puede utilizar el dispositivo **/dev/md0** como cualquier otra unidad de almacenamiento. Ejemplo:

```
mkfs.ext4 /dev/md0

mkdir /datos00

mount /dev/md0 /datos00

df -h

umount /datos00
```

Lo más recomendado es utilizar el nuevo dispositivo RAID para crear volúmenes lógicos.

Primero hay que crear una unidad física en el dispositivo RAID. Ejecute lo siguiente:

```
pvcreate /dev/md0
```

Lo anterior puede devolver una salida similar a la siguiente:

```
  Physical volume "/dev/md0" successfully created
```

Visualice el nuevo volumen físico ejecutando lo siguiente:

```
pvscan
```

Lo anterior puede devolver una salida similar a la siguiente:

```
  PV /dev/sda2   VG VolGroup        lvm2 [39,51 GiB / 0    free]
  PV /dev/md0                       lvm2 [8,00 GiB]
  Total: 2 [47,50 GiB] / in use: 1 [39,51 GiB] / in no VG: 1 [8,00 GiB]
```

Ejecute lo siguiente para generar un nuevo grupo de volumen:

```
vgcreate VGDatos00 /dev/md0
```

Lo anterior puede devolver una salida similar a la siguiente:

```
  Volume group "VGDatos00" successfully created
```

Ejecute lo siguiente para visualizar el nuevo grupo de volumen:

```
vgscan
```

Lo anterior puede devolver una salida similar a la siguiente:

```
  Reading all physical volumes.  This may take a while...
  Found volume group "VolGroup" using metadata type lvm2
  Found volume group "VGDatos00" using metadata type lvm2
```

Genere un volumen lógico denominado LVDatos00 dentro del grupo de volumen VGDatos00 utilizando cualquier porcentaje del espacio disponible. Se recomienda dejar siempre al menos un 10% libre para poder asignarlo sólo cuando sea necesario.

```
lvcreate -l 90%FREE VGDatos00 -n LVDatos00
```

Lo anterior puede devolver una salida similar a la siguiente:

```
  Logical volume "LVDatos00" created
```

Ejecute lo siguiente para visualizar el nuevo volumen lógico:

```
lvscan
```

Lo anterior puede devolver una salida similar a la siguiente:

```
  ACTIVE            '/dev/VolGroup/lv_root' [38,04 GiB] inherit
  ACTIVE            '/dev/VolGroup/lv_swap' [1,47 GiB] inherit
  ACTIVE            '/dev/VGDatos00/LVDatos00' [7,19 GiB] inherit
```

Ejecute lo siguiente para asignar formato al nuevo volumen lógico:

```
mkfs.ext4 /dev/VGDatos00/LVDatos00
```

Lo anterior puede devolver una salida similar a la siguiente:

```
mke2fs 1.41.12 (17-May-2010)
Etiqueta del sistema de ficheros=
Tipo de SO: Linux
Tamaño del bloque=4096 (bitácora=2)
Tamaño del fragmento=4096 (bitácora=2)
Stride=0 blocks, Stripe width=0 blocks
471424 nodos-i, 1885184 bloques
94259 bloques (5.00%) reservados para el superusuario
Primer bloque de datos=0
Número máximo de bloques del sistema de ficheros=1933574144
58 bloque de grupos
32768 bloques por grupo, 32768 fragmentos por grupo
8128 nodos-i por grupo
Respaldo del superbloque guardado en los bloques:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Escribiendo las tablas de nodos-i: hecho
Creating journal (32768 blocks): hecho
Escribiendo superbloques y la información contable del sistema de ficheros: hecho

Este sistema de ficheros se revisará automáticamente cada 23 montajes o
180 días, lo que suceda primero.  Utilice tune2fs -c o -i para cambiarlo.
```

Ejecute lo siguiente para generar un punto de montaje para asignar al nuevo volumen lógico:

```
mkdir -p /datos00
```

Ejecute lo siguiente para montar el nuevo volumen lógico en el nuevo directorio:

```
mount /dev/VGDatos00/LVDatos00 /datos00/
```

Ejecute lo siguiente para visualizar el sistema de archivos en el nuevo volumen lógico que se ha añadido en el sistema.

```
df -h
```

Lo anterior puede devolver una salida similar a la siguiente:

```
S.ficheros            Size  Used Avail Use% Montado en
/dev/mapper/VolGroup-lv_root
                       38G  4,3G   32G  13% /
tmpfs                 376M     0  376M   0% /dev/shm
/dev/sda1             485M   66M  394M  15% /boot
/dev/mapper/VGDatos00-LVDatos00
                      7,1G  145M  6,6G   3% /datos00
```

Para que el punto de montaje sea permanente y sea montado automáticamente con el siguiente inicio del sistema, edite el archivo **/etc/fstab**:

```
vi /etc/fstab
```

Añada la siguiente línea:

```
/dev/mapper/VGDatos00-LVDatos00 /datos00        ext4    defaults        1 2
```

Guarde y cierre el archivo. Verifique la configuración desmontando el volumen lógico y volviendo a montar éste del siguiente modo:

```
umount /datos00

mount /datos00
```

Lo anterior sólo debe devolver el símbolo de sistema.

Reinicie el sistema para verificar que todo quedó correctamente. Si el sistema reinició correctamente significa que esta primera parte del procedimiento se ha concluido el procedimiento.

Si más adelante necesita utilizar el espacio libre disponible en la unidad física, puede asignarlo con el sistema en funcionamiento y la partición montada sólo ejecutando lo siguiente:

```
lvextend -l +100%FREE /dev/mapper/VGDatos00-LVDatos00

resize2fs /dev/mapper/VGDatos00-LVDatos00
```

Compruebe el espacio disponible ejecutando lo siguiente:

```
df -h
```

Para este escenario, que está lejos de ser el más óptimo, si necesita hacer crecer el sistema de archivos se puede crear otro arreglo en RAID1 y repetir el procedimiento para configurar éste como unidad física, luego añadirlo a grupo de volumen y crecer el volumen lógico LVDatos00 para incrementar la capacidad de almacenamiento. **Sólo revise el siguiente ejemplo y en su lugar realice el procedimiento descrito más adelante para crear un RAID10**.

```
mdadm --create /dev/md1 --level=1 \
    --raid-devices=2 /dev/sde /dev/sdd

mdadm --detail --scan >> /etc/mdadm.conf

vi /etc/mdadm.conf

mdadm --detail

pvcreate /dev/md1

vgextend VGDatos00 /dev/md1

lvextend -l +90%FREE /dev/mapper/VGDatos00-LVDatos00

resize2fs /dev/mapper/VGDatos00-LVDatos00
```

12.2.2. Crear un arreglo tipo RAID10.

Un RAID10, con o sin LVM, es más eficiente en cuanto a rendimiento que un RAID1+LVM pues el rendimiento sigue siendo el de un RAID1 (espejo sin paridad).

Para un RAID10 requerirá un mínimo de 4 unidades de almacenamiento. Para el ejemplo a continuación se utilizarán 6 unidades de almacenamiento, donde se utilizarán 4 unidades activas en el arreglo y utilizarán 2 unidades de repuesto, las cuales serán utilizados automáticamente en cuanto falle cualquier otra unidad de almacenamiento. Tome en consideración que MDADM es incapaz de hacer crecer los arreglos en RAID10 y sólo permite agregar o reemplazar unidades de almacenamiento.

Ejecute lo siguiente para apagar el sistema:

```
poweroff
```

Añada 6 unidades de almacenamiento idénticas.

Encienda de nuevo el sistema.

Ejecute lo siguiente para generar un arreglo en RAID10 utilizando las primeras 4 unidades de almacenamiento recién agregadas.

```
mdadm  --create /dev/md1 --level=raid10 --raid-devices=4 \
    /dev/sdd /dev/sde /dev/sdf /dev/sdg
```

Espere a que el arreglo se construya. Se puede ver el estado de progreso ejecutando lo siguiente:

```
mdadm --detail /dev/md1
```

Lo anterior puede devolver una salida similar a la siguiente:

```
/dev/md1:
        Version : 1.2
  Creation Time : Tue Jun 11 23:30:10 2013
     Raid Level : raid10
     Array Size : 16768000 (15.99 GiB 17.17 GB)
  Used Dev Size : 8384000 (8.00 GiB 8.59 GB)
   Raid Devices : 4
  Total Devices : 4
    Persistence : Superblock is persistent

    Update Time : Tue Jun 11 23:30:49 2013
          State : active, resyncing
 Active Devices : 4
Working Devices : 4
 Failed Devices : 0
  Spare Devices : 0

         Layout : near=2
     Chunk Size : 512K

  Resync Status : 44% complete

           Name : 1
           UUID : 342944f9:8d1f5acf:2d72653b:a1f2f253
         Events : 8

    Number   Major   Minor   RaidDevice State
       0       8       48        0      active sync   /dev/sdd
       1       8       64        1      active sync   /dev/sde
       2       8       80        2      active sync   /dev/sdf
       3       8       96        3      active sync   /dev/sdg
```

Continúe hasta que se haya completado por completo la construcción del arreglo.

Tras unos minutos, ejecute lo siguiente para verificar que haya concluido el proceso de construcción del arreglo.

```
mdadm --detail /dev/md1
```

Lo anterior puede devolver una salida similar a la siguiente:

```
/dev/md1:
        Version : 1.2
  Creation Time : Tue Jun 11 23:30:10 2013
     Raid Level : raid10
     Array Size : 16768000 (15.99 GiB 17.17 GB)
  Used Dev Size : 8384000 (8.00 GiB 8.59 GB)
   Raid Devices : 4
  Total Devices : 4
    Persistence : Superblock is persistent

    Update Time : Tue Jun 11 23:31:36 2013
          State : active
 Active Devices : 4
Working Devices : 4
 Failed Devices : 0
  Spare Devices : 0

         Layout : near=2
     Chunk Size : 512K

           Name : 1
           UUID : 342944f9:8d1f5acf:2d72653b:a1f2f253
         Events : 18

    Number   Major   Minor   RaidDevice State
       0       8       48        0      active sync   /dev/sdd
       1       8       64        1      active sync   /dev/sde
       2       8       80        2      active sync   /dev/sdf
       3       8       96        3      active sync   /dev/sdg
```

Ejecute lo siguiente para agregar dos unidades de almacenamiento como repuestos:

```
mdadm --add /dev/md1 /dev/sdh
mdadm --add /dev/md1 /dev/sdi
```

Ejecute lo siguiente para observar el estado del arreglo y verificar que se han añadido todas las unidades de almacenamiento de repuesto inactivas.

```
mdadm --detail /dev/md1
```

Lo anterior puede devolver una salida similar a la siguiente:

```
/dev/md1:
        Version : 1.2
  Creation Time : Tue Jun 11 23:30:10 2013
     Raid Level : raid10
     Array Size : 16768000 (15.99 GiB 17.17 GB)
  Used Dev Size : 8384000 (8.00 GiB 8.59 GB)
   Raid Devices : 4
  Total Devices : 6
    Persistence : Superblock is persistent

    Update Time : Tue Jun 11 23:34:56 2013
          State : active
 Active Devices : 4
Working Devices : 6
 Failed Devices : 0
  Spare Devices : 2

         Layout : near=2
     Chunk Size : 512K

           Name : 1
           UUID : 342944f9:8d1f5acf:2d72653b:a1f2f253
         Events : 20

    Number   Major   Minor   RaidDevice State
       0       8       48        0      active sync   /dev/sdd
       1       8       64        1      active sync   /dev/sde
       2       8       80        2      active sync   /dev/sdf
       3       8       96        3      active sync   /dev/sdg

       4       8      112        -      spare   /dev/sdh
       5       8      128        -      spare   /dev/sdi
```

Guarde la información del arreglo recién creado en el archivo **/etc/mdadm.conf**.

```
mdadm --detail --scan >> /etc/mdadm.conf
```

Edite el archivo **/etc/mdadm.conf** y quite las líneas repetidas.

```
vi /etc/mdadm.conf
```

Este paso es importante, pues puede hacer que los arreglos repetidos sean imposibles de utilizar y el sistema sea incapaz de iniciar normalmente.

Una vez que esté todo configurado, proceda a crear otro volumen lógico:

```
pvcreate /dev/md1

pvscan

vgcreate VGDatos01 /dev/md1

vgscan

lvcreate -l 90%FREE VGDatos01 -n LVDatos01

lvscan

mkfs.ext4 /dev/mapper/VGDatos01-LVDatos01

mkdir -p /datos01

mount /dev/mapper/VGDatos01-LVDatos01 /datos01

df -h

umount /datos01
```

Edite el archivo **/etc/fstab**:

```
vi /etc/fstab
```

Añada la siguiente línea:

```
/dev/mapper/VGDatos01-LVDatos01 /datos01        ext4    defaults        1 2
```

Reinicie el sistema para verificar que todo quedó configurado correctamente.

Si el sistema reinició correctamente significa que se ha concluido el procedimiento.

12.2.3. Eliminar una unidad de almacenamiento de un arreglo.

Para eliminar una unidad de almacenamiento por falla o simplemente para probar, ejecute:

```
mdadm /dev/md1 --fail /dev/sdd --remove /dev/sdd
```

Lo anterior puede devolver una salida similar a la siguiente:

```
mdadm: set /dev/sdd faulty in /dev/md1
mdadm: hot removed /dev/sdd from /dev/md1
```

Ejecute lo siguiente para observar el detalle del arreglo donde observará que se reconstruye el arreglo con la unidad de almacenamiento de repuesto:

```
mdadm --detail /dev/md1
```

Lo anterior puede devolver una salida similar a la siguiente donde se podrá observar que en el estado se reporta arreglo limpio, degradado pero en recuperación:

```
/dev/md1:
        Version : 1.2
  Creation Time : Tue Jun 11 23:30:10 2013
     Raid Level : raid10
     Array Size : 16768000 (15.99 GiB 17.17 GB)
  Used Dev Size : 8384000 (8.00 GiB 8.59 GB)
   Raid Devices : 4
  Total Devices : 5
    Persistence : Superblock is persistent

    Update Time : Tue Jun 11 23:48:05 2013
          State : clean, degraded, recovering
 Active Devices : 3
Working Devices : 5
 Failed Devices : 0
  Spare Devices : 2

         Layout : near=2
     Chunk Size : 512K

 Rebuild Status : 67% complete

           Name : 1
           UUID : 342944f9:8d1f5acf:2d72653b:a1f2f253
         Events : 36

    Number   Major   Minor   RaidDevice State
       5       8      128        0      spare rebuilding   /dev/sdi
       1       8       64        1      active sync   /dev/sde
       2       8       80        2      active sync   /dev/sdf
       3       8       96        3      active sync   /dev/sdg

       4       8      112        -      spare   /dev/sdh
```

Ejecute lo siguiente para añadir al arreglo la unidad anteriormente eliminada, simulando que se trata de una unidad de almacenamiento nueva:

```
mdadm --zero-superblock /dev/sdd
mdadm --add /dev/md1 /dev/sdd
```

Lo anterior puede devolver una salida similar a la siguiente:

```
mdadm: added /dev/sdd
```

Ejecute lo siguiente para comprobar que la unidad de almacenamiento se ha agregado como unidad de repuesto:

```
mdadm --detail /dev/md1
```

Lo anterior puede devolver una salida similar a la siguiente:

```
/dev/md1:
        Version : 1.2
  Creation Time : Tue Jun 11 23:30:10 2013
     Raid Level : raid10
     Array Size : 16768000 (15.99 GiB 17.17 GB)
  Used Dev Size : 8384000 (8.00 GiB 8.59 GB)
   Raid Devices : 4
  Total Devices : 6
    Persistence : Superblock is persistent

    Update Time : Tue Jun 11 23:50:09 2013
          State : clean
 Active Devices : 4
Working Devices : 6
 Failed Devices : 0
  Spare Devices : 2

         Layout : near=2
     Chunk Size : 512K

           Name : 1
           UUID : 342944f9:8d1f5acf:2d72653b:a1f2f253
         Events : 46

    Number   Major   Minor   RaidDevice State
       5       8      128        0      active sync   /dev/sdi
       1       8       64        1      active sync   /dev/sde
       2       8       80        2      active sync   /dev/sdf
       3       8       96        3      active sync   /dev/sdg

       4       8      112        -      spare   /dev/sdh
       6       8       48        -      spare   /dev/sdd
```

12.2.4. Eliminar un arreglo del sistema.

Para eliminar un arreglo, primero desmonte el sistema de archivos. En el siguiente ejemplo realizará con el arreglo configurado como /dev/md0.

```
umount /datos00
```

Edite el archivo **/etc/fstab**:

```
vi /etc/fstab
```

Elimine la linea que corresponda al sistema de archivos contenido en el arreglo.

Si fuese el caso, se debe eliminar el volumen lógico que pudisese contener. Ejemplo:

```
lvremove LVDatos00
```

Ejecute lo siguiente para eliminar el grupo de volumen:

```
vgremove VGDatos00
```

Ejecute lo siguiente para detener el arreglo:

```
mdadm --stop /dev/md0
```

Edite el archivo **/etc/mdadm.conf**:

```
vi /etc/mdadm.conf
```

Elimine la línea que correspondía al arreglo /dev/md0.

Verifique que se ha eliminado el arreglo ejecutando:

```
mdadm --detail --scan
```

Ejecute lo siguiente para poder volver a utilizar las unidades de almacenamiento saludables para añadirlas a otro arreglo o bien como unidades físicas en un volumen lógico:

```
mdadm --zero-superblock /dev/sdb
mdadm --zero-superblock /dev/sdc
```

12.3. Otras alternativas para gestionar MDADM.

Cabe señalar que Webmin incluye una excelente herramienta de administración para arreglos de disco con MDADM.

Si utiliza **CentOS** o **Red Hat™ Enterprise Linux**, descargue el archivo de configuración del almacén YUM de **AlcanceLibre.org** ejecutando lo siguiente:

```
wget http://www.alcancelibre.org/al/server/AL-Server.repo \
    -O /etc/yum.repos.d/AL-Server.repo
```

Instale el paquete ejecutando lo siguiente

```
yum -y install webmin
```

Una vez concluida la instalación del paquete, para poder acceder hacia la interfaz de Webmin es necesario abrir en el muro cortafuegos el acceso hacia el puerto 10000 por TCP. Ejecute lo siguiente para modificar el cortafuegos predeterminado del sistema:

```
iptables -A INPUT -m state --state NEW -m tcp -p tcp \
    --dport 10000 -j ACCEPT
```

Ejecute lo siguiente para guardar los cambios en la configuración del muro cortafuegos:

```
service iptables save
```

Acceda hacia *https://nombre.dominio.tld:10000/* utilizando cualquier navegador para interfaz gráfica. Ingrese como **root** y descubra que todos los procedimientos descritos en este documento se pueden hacer más fácilmente desde el módulo **Linux RAID** de la sección de **Hardware** de **Webmin**. El objetivo de este documento es que usted conozca cómo funciona todo por debajo de lo que puede hacer **Webmin** y pueda prescindir de dicha interfaz en cualquier circunstancia que así lo requiera.

13. Optimización de sistemas de archivos ext3 y ext4.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales (incluyendo su publicación, a través de cualquier medio, por entidades con fines de lucro). c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en castellano. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

13.1. Introducción.

Cuando se trabaja con servidores y estaciones de trabajo, con instalaciones de **Ubuntu**, **CentOS**, **Red Hat** o **Fedora** y se busca optimizar el uso del disco duro de sistemas de archivos en formato Ext3 o Ext4, hay ajustes que pueden mejorar el desempeño de manera significativa.

13.1.1. Acerca de Ext3.

Ext3 (*third extended filesystem* o tercer sistema de archivos extendido) se diferencia de **ext2** en que trabaja con registro por diario (*journaling*) y porque utiliza un árbol binario balanceado (árbol **AVL**, creado por los matemáticos rusos Georgii **A**delson-**V**elskii y Yevgeniy **L**andis) y también por incorporar el método **Orlov** de asignación para bloques de disco (el mismo que se gestiona a través de los mandatos **lsattr** y **chattr**). Además **ext3** permite ser montado y utilizado, como si fuera **ext2** y actualizar desde **ext2** hacia **ext3** sin necesidad de formatear la partición y, por tanto, sin perder los datos almacenados en ésta. Es el sistema de archivos predeterminado en **CentOS 5** y **Red Hat Enterprise Linux 5**.

13.1.2. Acerca de Ext4.

Ext4 (*fourth extended filesystem* o cuarto sistema de archivos extendido) es un sistema de archivos con registro por diario, publicado por Andrew Morton como una mejora compatible con el formato Ext3 el 10 de octubre de 2006. El 25 de diciembre de 2008 se publicó la versión 2.6.28 del núcleo de Linux, la cual eliminó la etiqueta *experimental* de código de Ext4. Las mejoras respecto de Ext3 incluyen, entre otras cosas, el soporte de volúmenes de hasta 1024 PiB, soporte añadido de *extents* (conjunto de bloques físicos contiguos), menor uso de recursos de sistema, mejoras sustanciales en la velocidad de lectura y escritura y verificación más rápida con **fsck**. Es el sistema de archivos predeterminado en **CentOS 6** y **Red Hat Enterprise Linux 6**.

13.1.3. Acerca del registro por diario (journaling).

El registro por diario (*journaling*) es un mecanismo por el cual un sistema de archivos implementa transacciones. Consiste en un registro en el que se almacena la información necesaria para restablecer los datos dañados por una transacción en caso de que ésta falle, como puede ocurrir durante una interrupción de energía.

13.2. Procedimientos

Para determinar que dispositivos corresponden a las particiones en el disco duro, se utiliza el mandato **df**. Ejemplo:

```
[root@servidor ~]# df
S.archivos         Bloques de 1K   Usado    Dispon Uso% Montado en
/dev/hda2             19283024  17279260   1207584  94% /
/dev/sda1                77749     21905     51830  30% /boot
/dev/sdb1             17496684  10618980   5988912  64% /home
/dev/hda5             54158844  41284544  11223624  79% /var/ftp
/dev/sda2             15352348   4874232   9698164  34% /home/rpmbuild
tmpfs                   777732         0    777732   0% /dev/shm
```

Una vez determinados que dispositivos corresponden a las diferentes particiones, pueden aplicarse varios métodos de optimización.

13.2.1. Utilizando el mandato e2fsck.

El mandato **e2fsck** se utiliza regularmente para revisar y reparar, particiones con formato **ext2**, **ext3** y **ext4**. Incluye la opción **-D** que realiza la optimización de directorios en el sistema de archivos. La optimización de todos los directorios de una partición consiste en volver a posicionar (*reindexing*) los directorios, cuando el sistema de archivos incluye soporte para tal, o volviendo a acomodar y comprimiendo directorios. La opción **-D** se debe utilizar junto con la opción **-f** para forzar la verificación de la partición del disco duro.

Para optimizar una partición cuyo formato es **ext3** o **ext4**, es indispensable que ésta esté desmontada. Para poder desmontar una partición es indispensable que el sistema funcione sin procesos haciendo uso de contenidos en dicha partición. Puede utilizarse el mandato **lsof** para determinar ésto y así definir que es lo que se debe detener momentáneamente.

Si el sistema funciona sin procesos haciendo uso de contenidos en la partición, se puede seguir el procedimiento ejemplificado a continuación con el dispositivo **/dev/sda3** que en este particular ejemplo corresponde a la partición para **/home**:

```
umount /home
e2fsck -f -D /dev/sda3
```

La salida puede devolver algo similar a lo siguiente:

```
[root@m100 SPECS]# e2fsck -D -f /dev/sda3
e2fsck 1.39 (29-May-2006)
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 3A: Optimizing directories
Pass 4: Checking reference counts
Pass 5: Checking group summary information
/home: ***** FILE SYSTEM WAS MODIFIED *****
/home: 13/5244736 files (7.7% non-contiguous), 208319/5243214 blocks
```

Una vez terminado el procedimiento, se pueden volver a montar las particiones optimizadas.

En el caso de tratarse de particiones que sea imposible desmontar por encontrarse en uso, puede utilizarse el disco de instalación de CentOS, Fedora, Red Hat Enterprise Linux, openSUSE y SuSE Linux Enterprise, en modo de rescate o bien un Disco Vivo (*LiveCD*), desmontando las particiones que se quieran optimizar antes de proceder con el mandato **e2fsck -f -D**.

13.2.2. Opciones de montado.

Los sistemas de archivos ext3 y ext4 permiten tres opciones que mejoran el desempeño del sistema de archivos. Todas se especifican en la columna de opciones de los dispositivos en el archivo **/etc/fstab**.

```
dispositivo   punto de montaje    formato    opciones    a b
```

De la descripción anterior, **a** define si la partición se verifica con cada inicio del sistema y **b** define la prioridad de montaje. Ejemplo del contenido del archivo **/etc/fstab**:

```
#
# /etc/fstab
# Created by anaconda on Mon Aug 22 14:39:31 2011
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=a3b3ebcd-e342-43fb-bc33-adf4d1e409ff /         ext4   defaults       1 1
UUID=32932fc8-0e4f-4a68-80a0-28d873a15f87 /boot     ext4   defaults       1 2
UUID=68ea9cb2-959a-4df1-8d3f-8e8554db4925 /home     ext4   defaults       1 2
UUID=238e532b-250c-4a80-87a3-3aecc9715795 /tmp      ext4   defaults       1 2
UUID=03df5f97-5c88-4883-97f1-5091940fa30e swap      swap   defaults       0 0
tmpfs                                     /tmp      tmpfs  defaults       0 0
tmpfs                                     /dev/shm  tmpfs  defaults       0 0
devpts                                    /dev/pts  devpts gid=5,mode=620 0 0
sysfs                                     /sys      sysfs  defaults       0 0
proc                                      /proc     proc   defaults       0 0
```

Edite el archivo /etc/fstab:

```
vi /etc/fstab
```

13.2.2.1. Opciones noatime y nodiratime (eliminar tiempos de acceso).

Es la forma más rápida y fácil, de lograr mejoras en el desempeño. Esta opción impide se actualice los tiempos de acceso de los *inodos* (nodos índice), los cuales realmente son poco utilizados por la mayoría de los usuarios. Esto permite mejor desempeño en servidores de noticias, servidores de archivos, servidores FTP y servidores **HTTP**, pues permite un más rápido acceso hacia el sistema de archivos. En computadoras portátiles permite reducir, de manera considerable, la cantidad de procesos de **E/S** o **E**ntrada y **S**alida (**I/O** o **I**nput/**O**utput), del disco duro. Equivale a utilizar **chattr +A**, pero aplicado a todos los datos de la partición. La opción **nodiratime**, que elimina los tiempos de acceso de los directorios, complementa a la opción **noatime**.

En el siguiente ejemplo, se configurará la opción **noatime** para el volumen lógico correspondiente a **/var/www** en el archivo **/etc/fstab**.

```
/dev/mapper/vg_01-LogVol03  /var/www  ext4  defaults,noatime,nodiratime  1 2
```

13.2.2.2. Opción commit (consignación de cambios).

Esta opción controla el tiempo que se utilizará entra cada operación sincronización (**sync**) de datos y *metadatos* en una partición. El **tiempo predeterminado** es de **5 segundos**. Puede incrementarse ligeramente para mejorar el desempeño, tomando en cuenta que si se específica demasiado tiempo y ocurre una interrupción de energía antes de hacer una operación de sincronización (**sync**), se perderán los datos más recientes con los que se haya trabajado. Esta opción **sólo se recomienda si se dispone de un sistema de respaldo de energía confiable**.

En el siguiente ejemplo, se configurará la opción **commit** con el valor equivalente a **8 segundos** para el volumen lógico correspondiente a **/var/www** en el archivo **/etc/fstab**.

```
/dev/mapper/vg_01-LogVol03  /var/www  ext4  defaults,noatime,nodiratime,commit=30  1 2
```

13.2.2.3. Opción data (datos).

Nota: Debido a que se debe desmontar y volver a montar para aplicar los cambios, se requiere que la partición a optimizar **esté sin utilizar, por lo cual se recomienda realizar los procedimiento desde un disco de rescate o bien iniciando el sistema en nivel de ejecución 1 (mono-usuario) o bien realizar las modificaciones y reiniciar el sistema.**

Esta opción permite tres posibles valores:

- **ordered**: Es el valor predeterminado. Escribe los datos asociados a los *metadatos* primero en el sistema de archivos antes de hacerlo en el registro por diario. Si la prioridad es garantizar la integridad de datos o bien se carece de un sistema de respaldo de energía confiable, es la opción que debe utilizarse.
- **journal**: Es lo opuesto a **ordered**. Obliga a escribir primero los datos en el registro por diario y luego en el sistema de archivos, por lo cual utiliza un registro por diario más grande y el cual, por lo tanto, demora más tiempo en recuperarse en caso de una falla del sistema o interrupción de energía. Éste es, evidentemente, el método más lento en la mayoría de los casos, salvo que se realicen operaciones de lectura y escritura, al mismo tiempo, como ocurre con las bases de datos.
- **writeback**: Hace que el sistema de archivos se comporte de manera similar a **XFS**. Sin preservar el ordenamiento al escribir en el disco, de modo que las **consignaciones de cambios** (*commits*) en el registro por diario puede ocurrir antes de la escritura en el sistema de archivos. Este método es **el más rápido** porque sólo los *metadatos* se almacenan en el registro por diario, pero puede ocasionar que se muestren datos viejos después de una falla del sistema o interrupción de energía. Sólo se recomienda si se dispone de un sistema de respaldo de energía confiable o bien si en la partición configurada con este formato de registro por diario **hay cambios poco frecuentes en los datos** (como el caso de **/boot**, **/**, **/usr**, **/opt**, **/usr/local**, y, en algunos, escenarios para **/var/www**) o bien particiones para temporales o caches (como **/tmp**, **/var/tmp** y **/var/cache**. Poco recomendado para particiones donde hay cambios frecuentes en los datos almacenados, como ocurre con **/home** o **/var**, **/var/lib** o **/var/spool**.

Edite el archivo **/etc/fstab**:

```
vi /etc/fstab
```

En el siguiente ejemplo se configurará en el archivo **/etc/fstab** el volumen lógico correspondiente a **/var/www** con la opción **data** con el valor **writeback** y el volumen lógico correspondiente a **/var/lib** con la opción **data** y el valor **journal**.

```
/dev/mapper/vg_01-LogVol03   /var/www   ext4   defaults,data=writeback    1 2
/dev/mapper/vg_01-LogVol04   /var/lib   ext4   defaults,data=journal      1 2
```

Si se utiliza **CentOS 6**, cualquier versión reciente de **Fedora™** o **Red Hat™ Enterprise Linux 6**, el formato del registro por diario **se actualiza automáticamente** al reiniciar el sistema o bien tras desmontar y volver a montar el sistema de archivos que se haya modificado. Para las versiones anteriores de estos sistemas operativos, antes de desmontar y volver a montar o bien reiniciar el sistema, es necesario convertir los registros por diario a su nuevo formato utilizando el mandato **tune2fs**. En el siguiente ejemplo se cambia el formato del registro por diario **writeback** al volumen lógico **/dev/mapper/vg_01-LogVol0** que correspondería al directorio **/var/www** del ejemplo anterior:

```
tune2fs -o journal_data_writeback /dev/mapper/vg_01-LogVol03
```

En el caso donde se desea cambiar el formato del registro por diario a **journal**, considerando el ejemplo descrito arriba, donde el volumen lógico **/dev/mapper/vg_01-LogVol04** corresponde al directorio **/var/lib**, se ejecutaría algo similar a lo siguiente:

```
tune2fs -o journal_data /dev/mapper/vg_01-LogVol04
```

Para aplicar los cambios, sin correr el riesgo de reiniciar con errores de sintaxis en el archivo **/etc/fstab** que impedirían montar las particiones configuradas, asumiendo que el sistema está en el nivel de ejecución 1 (mono-usuario), se puede utilizar el mandato **umount** para desmontar la partición a modificar y posteriormente el mandato **mount** para volver a montarla. Ejemplos:

```
umount /var/www
umount /var/lib
mount /var/www
mount /var/lib
```

Utilizar el mandato **mount** con la opción **-o remount** siempre devolverá un error de opción incorrecta. Esta es la razón por la cual se desmontan y montan las particiones, para cambiar el tipo de registro por diario de las particiones.

Si lo anterior devuelve el símbolo de sistema sin errores, significa que las opciones **se aplicaron correctamente** y que el sistema puede ser reiniciado con toda seguridad en el momento que se considere apropiado.

Para revertir el cambio y volver a utilizar el formato **ordered**, se edita nuevamente el archivo **/etc/fstab**:

```
vi /etc/fstab
```

Y se elimina la opción data y su valor correspondiente del archivo **/etc/fstab**:

```
/dev/mapper/vg_01-LogVol03   /var/www   ext4   defaults              1 2
/dev/mapper/vg_01-LogVol04   /var/lib   ext4   defaults              1 2
```

Y se ejecuta el mandato **tune2fs** con la opción **-o** y el valor **journal_data_ordered** y el volumen lógico o partición como argumento. En el siguiente ejemplo se regresa al formato **ordered** a los volúmenes lógicos de los ejemplos anteriores:

```
tune2fs -o journal_data_ordered /dev/mapper/vg_01-LogVol03
tune2fs -o journal_data_ordered /dev/mapper/vg_01-LogVol04
```

Para aplicar los cambios, sin correr el riesgo de reiniciar con errores de sintaxis en el archivo **/etc/fstab** que impedirían montar las particiones configuradas, asumiendo que el sistema está en el nivel de ejecución 1 (mono-usuario), se puede utilizar el mandato **umount** para desmontar la partición a modificar y posteriormente el mandato **mount** para volver a desmontarlas. Ejemplos:

```
umount /var/www
umount /var/lib
mount /var/www
mount /var/lib
```

13.2.3. Convirtiendo particiones de Ext3 a Ext4.

En **CentOS 6**, versiones recientes de **Fedora™** y **Red Hat Enterprise Linux 6** el formato predeterminado en las particiones es Ext4, por lo cual es innecesario convertir de Ext3 a Ext4.

Ext4 ha demostrado ser un sistema de archivos con mucho mejor desempeño que Ext3. Si sólo se necesita hacer pruebas, es posible montar una partición Ext3 como si fuese Ext4, modificando el archivo **/etc/fstab**, aunque se carecerá de muchas de las mejoras de Ext4.

Instalando los paquetes correspondientes, CentOS 5.5 y versiones posteriores, incluye el soporte necesario para convertir al formato Ext4 las particiones Ext3, preservando los datos originales en el sistema de archivos, con la única restricción de que jamás se deberá convertir a Ext4 las particiones que correspondan **/boot** y **/**, debido a que en CentOS 5 y Red Hat Enterprise Linux 5 la versión de Grub, el gestor de arranque, carece de soporte para iniciar desde particiones Ext4.

Es muy importante realizar un respaldo de información relevante antes de proceder, por si acaso algo saliese mal.. Si se utiliza **CentOS 5** o **Red Hat Enterprise Linux 5**, jamás se deben convertir a Ext4 las particiones que correspondan a **/boot** y **/**.

En **CentOS 5** o **Red Hat Enterprise Linux 5**, para poder utilizar el formato Ext4 en cualquier otra partición, se requiere que el sistema tenga instalado el paquete **e4fsprogs**:

```
yum -y install e4fsprogs
```

Este paquete incluye las herramientas necesarias para gestionar particiones Ext4, como son **e4fsck**, **e4label**, **mke4fs**, **mkfs.ext4** y **dumpe4fs**, entre otras herramientas.

A partir de este punto y con el objetivo de realizar pruebas, sólo será necesario editar el archivo **/etc/fstab** y modificar la configuración de cualquier partición (**excepto las que correspondan a /boot y /**) y cambiar **ext3** por **ext4**. Hasta aquí, es posible revertir el cambio volviendo a editar el archivo **/etc/fstab** y volviendo a definir **ext3** como formato de la partición modificada.

Para convertir una partición por completo a Ext4, **lo cual haría que de modo irreversible jamás se pueda volver a montar como Ext3**, debe desmontarse primero la partición a convertir y posteriormente utilizar el mandato tune4fs con las opciones **-O extents,uninit_bg,dir_index**. En el siguiente ejemplo se aplica el mandato **tune4fs** a la partición **/dev/sda7**, que correspondería a **/tmp**, para convertirla a Ext4.

```
umount /tmp
tune4fs -O extents,uninit_bg,dir_index /dev/sda7
```

Utilice el mandato **fsck.ext4** para verificar el sistema de archivos de la partición y así completar los cambios necesario. El mandato **fsck.ext4** debe utilizarse con las opciones **-fyD** (forzar verificación, contestar si a todas las modificaciones necesarias y optimizar directorios).

```
fsck.ext4 -fyD /dev/sda7
```

Si la partición está en uso, como sería el caso de las correspondientes a **/usr** y/o **/var**, será necesario hacer lo anterior desde un disco vivo o bien un disco de rescate. El **modo de rescate** del disco de instalación de CentOS, versión 5.5 en adelante, incluye también soporte básico para Ext4, aunque carece de soporte para convertir particiones de Ext3 a Ext4 a través del mandato **tune2fs** y carece de mandato **tune4fs**. Por tanto, el intérprete de mandatos del modo de rescate del disco de instalación de CentOS 5.5 sólo permitirá verificar y reparar, particiones Ext4 a través del mandato **fsck.ext4**.

En el archivo **/etc/fstab** se reemplaza **LABEL=/tmp** por el nombre real del dispositivo y **ext3** por **ext4**.

```
LABEL=/                 /                       ext3    defaults        1 1
LABEL=/boot             /boot                   ext3    defaults        1 2
/dev/sda7               /tmp                    ext4    defaults        1 2
LABEL=SWAP-hda3         swap                    swap    defaults        0 0
tmpfs                   /dev/shm                tmpfs   defaults        0 0
devpts                  /dev/pts                devpts  gid=5,mode=620  0 0
sysfs                   /sys                    sysfs   defaults        0 0
proc                    /proc                   proc    defaults        0 0
```

Ext4 utiliza **UUID** (*Universally Unique Identifier* o Identificador Universalmente Único) en lugar de etiquetas. El **UUID** se puede determinar utilizando el mandato **blkid** del siguiente modo:

```
blkid /dev/sda7
```

Lo cual devolvería algo similar a lo siguiente:

```
/dev/sda7: LABEL="/tmp" UUID="238e532b-250c-4a80-87a3-3aecc9715795" TYPE="ext4"
```

Con esta información, el archivo **/etc/fstab** quedaría del siguiente modo:

```
LABEL=/                                 /       ext4    defaults        1 1
LABEL=/bot                              /boot   ext4    defaults        1 2
LABEL=/home                             /home   ext4    defaults        1 2
UUID=238e532b-250c-4a80-87a3-3aecc9715795   /tmp    ext4    defaults    1 2
LABEL=SWAP-sda3                         swap    swap    defaults        0 0
tmpfs                   /dev/shm        tmpfs   defaults        0 0
devpts                  /dev/pts        devpts  gid=5,mode=620  0 0
sysfs                   /sys            sysfs   defaults        0 0
proc                    /proc           proc    defaults        0 0
```

Monte de nuevo la partición.

```
mount /tmp
```

Ext3 utiliza una *cartografía* de mapas de bits. Ext4 se caracteriza por el uso de *extents*. Para completar el procedimiento, hay que migrar los archivos y directorios de la partición para que utilicen *extents*. Los archivos se pueden ir migrando con las subsecuentes escrituras en disco, pero mucho del contenido estático, como binarios y bibliotecas compartidas, pueden pasar meses antes de poder ser convertidos.

Una forma de convertir todo de una vez, es utilizar el mandato **chattr** para añadir el atributo de *extents* a todos los archivos y directorios de una partición en particular.

```
find /tmp -xdev -type f -print0 | xargs -0 chattr +e
find /tmp -xdev -type d -print0 | xargs -0 chattr +e
```

Desmonte de nuevo la partición.

```
umount /tmp
```

Con la finalidad de prevenir cualquier problema, vuelva a verificar la partición.

```
fsck.ext4 -fyD /dev/sda7
```

Para finalizar el procedimiento, monte de nuevo la partición.

```
mount /tmp
```

13.2.4. Eliminando el registro por diario (*journal*) de Ext4.

13.2.4.1. Advertencias.

Este procedimiento aplica exclusivamente a las particiones con formato Ext4. **El formato Ext3 carece de soporte para funcionar sin registro por diario**.

Eliminar el registro por diario implica perder la tecnología lo que garantiza la integridad de los datos de una partición en caso de una interrupción de energía o una falla general del sistema. Sólo se recomienda eliminar el registro por diario en los casos donde se dispone de un buen respaldo de energía (equipos portátiles y ultra-portátiles, por ejemplo), un sistema operativo estable, y/o se tienen particiones asignadas a directorios donde la información es poco relevante (como /tmp, /var/tmp o /var/cache). Este procedimiento está totalmente contraindicado en servidores o bien donde se requiera una garantía absoluta de integridad de datos.

Hay que considerar además que la mejoría obtenida puede ser apenas perceptible, y, muy probablemente, sólo amerite eliminar el registro por diario en particiones en unidades de estado sólido (SSD).

Es importante también realizar un respaldo de información relevante antes de proceder, por si acaso algo saliese mal..

13.2.4.2. Procedimientos.

Asumiendo que se dispone de una partición **/dev/sda7**, que en el ejemplo corresponde a **/tmp**, que fue previamente convertida a Ext4, utilizando el método descrito en este mismo documento o bien que ya tiene formato Ext4, se debe desmontar la partición:

```
umount /tmp
```

Para eliminar el registro por diario de la partición **/dev/sda7** en **CentOS 5** o **Red Hat Enterprise Linux 5**, se requiere ejecutar el mandato **tune4fs**, de la siguiente forma:

```
tune4fs -O ^has_journal /dev/sda7
```

Para eliminar el registro por diario de la partición **/dev/sda7** en **CentOS 6** o **Red Hat Enterprise Linux 6**, se requiere ejecutar el mandato **tune2fs**, de la siguiente forma:

```
tune2fs -O ^has_journal /dev/sda7
```

El símbolo ^ (acento circunflejo) significa que se elimina una opción. En este caso la opción eliminada fue **has_journal**, que es las responsable del registro por diario.

Sin importar la versión de sistema operativo o anterior requiere utilizar en seguida el mandato **fsck**, con las opciones **-pDf** (reparar automáticamente lo que sea necesario y que prescinda de interacción humana, optimizar re-ordenando directorios y forzar verificación) a fin de **realizar correcciones importantes e indispensables** en el sistema de archivos.

```
fsck.ext4 -pDf /dev/sda7
```

Eliminar el registro por diario de una partición ext4 hace que irremediablemente sea imposible leer el **UUID** de la partición, por lo cual invariablemente hay que editar el archivo **/etc/fstab** y establecer el nombre real del dispositivo en lugar del **UUID**:

```
LABEL=/                 /                       ext3    defaults        1 1
LABEL=/boot             /boot                   ext3    defaults        1 2
/dev/sda7               /tmp                    ext4    defaults        1 2
tmpfs                   /dev/shm                tmpfs   defaults        0 0
devpts                  /dev/pts                devpts  gid=5,mode=620  0 0
sysfs                   /sys                    sysfs   defaults        0 0
proc                    /proc                   proc    defaults        0 0
LABEL=SWAP-hda3         swap                    swap    defaults        0 0
```

El procedimiento concluye una vez modificado el archivo **/etc/fstab**. Vuelva a montar la partición para verificar que todo funcione correctamente.

```
mount /tmp
```

La mejoría será apenas perceptible, pero brindará el máximo rendimiento posible para el sistema de archivos Ext4, superando incluso el desempeño en cuanto a velocidad de Ext2.

En un equipo con una partición **/tmp** con registro por diario y la misma partición **/tmp**, sin registro por diario, la **escritura** de 1 GB de información demoró lo siguiente:

```
                                                real    0m9.796s
/tmp con registro por diario                    user    0m0.444s
                                                sys     0m4.441s

                                                real    0m8.978s
/tmp sin registro por diario                    user    0m0.487s
                                                sys     0m3.811s
```

Como pude verse, la diferencia es **muy poca**, pero significativa.

En el dado caso que se quiera volver a utilizar el registro por diario, sólo basta con volver a iniciar con el disco vivo, abrir una terminal y ejecutar lo siguiente.

```
su -l
umount /home
tune2fs -O has_journal /dev/sda7
fsck -pDf /dev/sda7
mount /home
```

13.3. Bibliografía.

- http://www.debian-administration.org/articles/643

14. Cifrado de particiones con LUKS.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

14.1. Introducción.

LUKS (**L**inux **U**nified **K**ey **S**etup-on-disk-format) es una implementación muy sencilla de utilizar para la gestión de particiones y unidades de almacenamiento cifradas en GNU/Linux. Se recomienda su uso en dispositivos móviles, computadoras portátiles y dispositivos de almacenamiento cuya información se desee proteger en caso de extravío o robo.

Las particiones o unidades de almacenamiento externo cifradas con **LUKS**, pueden ser utilizadas desde Windows utilizando **FreeOTFE**.

Este documento describe los procedimientos para cifrar una partición de disco duro, asignada al punto de montaje **/datos**. **Cabe señalar que el procedimiento hará que todos los datos de esta partición se pierdan**. Si la partición contiene datos de algún tipo, se debe respaldar todo antes de proceder y verificar que el respaldo esté completo e integro, para luego restaurar estos datos después de terminar el procedimiento.

14.2. Equipamiento lógico necesario.

14.2.1. En CentOS, Fedora y Red Hat Enterprise Linux.

Por lo general el paquete **cryptsetup-luks** viene instalado de manera predeterminada. Sí acaso fuese necesario, instalar el paquete correspondiente con el mandato **yum**:

```
yum -y install cryptsetup-luks
```

14.2.2. En openSUSE y SUSE Linux Enterprise.

Por lo general el paquete **cryptsetup** viene instalado de manera predeterminada. Sí a caso fuese necesario, instalar el paquete correspondiente con el mandato **yast**:

```
yast -i cryptsetup
```

14.3. Procedimientos.

A fin de evitar contratiempos, conviene realizar todos los procedimientos desde el nivel de ejecución 1 (mono usuario). Como root ejecute:

```
init 1
```

Antes de proceder, es muy importante cerciorarse de qué dispositivo se va a utilizar para el procedimiento. De ser necesario y sí acaso estuviese montada, utilice el mandato **df** para determinar que dispositivo corresponde a la partición que se desea cifrar.

```
df -h
```

Respalde todos los datos de la partición que necesite cifrar. Copie o mueva, los datos hacia otro dispositivo de almacenamiento. **El procedimiento eliminará, de manera inevitable, todo el contenido actual de dicha partición**.

```
mkdir -p /var/respaldo/datos/
tar cpf /var/respaldo/datos.tar /datos/
```

Antes de continuar, será una buena idea que verifique y compruebe que el respaldo es confiable.

14.3.1. Cifrado de una partición existente en CentOS, Fedora™ y Red Hat™ Enterprise Linux.

Salvo que se realice el procedimiento desde la instalación del sistema operativo —donde sólo se requiere habilitar la casilla de Cifrar partición— estas distribuciones carecen de una herramienta para hacer el procedimiento fácil. Es necesario hacer uso del intérprete de mandatos.

Una vez hecho el respaldo y que haya verificado que el respaldo es confiable, desmonte la partición que se pretende cifrar:

```
umount /datos
```

El siguiente paso **es opcional**, pero se recomienda llevarlo a cabo, pues mejora el cifrado al llenar previamente la partición con datos aleatorios. Debe tomarse en consideración que &mdahs;dependiendo del tamaño de la partición— ésto puede demorar varias horas o incluso días.

```
dd if=/dev/urandom of=/dev/sdaX bs=4096
```

La partición a utilizar se debe preparar con el mandato **cryptsetup**, con las opciones **--verbose** (para obtener una salida más descriptiva en caso de problemas), **--verify-passphase** (para asignar una frase de acceso o bien una contraseña), **luksFormat** para dar formato en LUKS y el nombre del dispositivo.

```
cryptsetup --verbose --verify-passphrase luksFormat /dev/sdaX
```

Lo anterior requerirá responder explícitamente con **YES**, en mayúsculas, que se desea proceder y que se está consciente que se perderán todos los datos actuales de la partición. A continuación, se pulsa la tecla **ENTER** y se ingresa la nueva frase o bien la nueva contraseña, que se pretenda asignar.

Una vez realizado lo anterior, para poder hacer uso de la nueva partición cifrada, se utiliza el mandato **cryptsetup** con la opción **luksOpen**, indicando el dispositivo que corresponde a la partición que se acaba de cifrar y el nombre que se quiera asignar a ésta en el planificador de dispositivos (*device mapper*).

```
cryptsetup luksOpen /dev/sdaX datos
```

Lo anterior crea un nuevo dispositivo denominado **/dev/mapper/datos**.

Para que el sistema operativo pueda utilizarlo, este nuevo dispositivo requiere ser formateado. En el siguiente ejemplo se da formato en ext4 a **/dev/mapper/datos**:

```
mkfs.ext4 /dev/mapper/datos
```

A fin de que el sistema solicite automáticamente la frase de acceso o bien la contraseña, al volver iniciar el sistema, se crea o edita el archivo **/etc/crypttab**:

```
vim /etc/crypttab
```

Dentro de éste, se define, en el primer campo, el nombre que se quiera utilizar para el planificador de dispositivos (*device mapper*), en el segundo campo se define el nombre del dispositivo que se cifró y en el tercer campo se define **none**. De manera opcional, aunque poco recomendado, se puede especificar la frase de acceso o bien la contraseña o bien un archivo que contenga ésta, en lugar de **none** para que el sistema inicie sin necesidad de que el administrador ingrese la frase de acceso o bien la contraseña.

```
datos   /dev/sdaX       none
```

A fin de que el sistema operativo monte automáticamente el dispositivo, se edita el archivo **/etc/fstab**:

```
vim /etc/fstab
```

Y se añade lo siguiente o bien se reemplaza el nombre del dispositivo anterior (UUID=xxxxxxxxxxxx, /dev/sdaX o LABEL=/datos, dependiendo de la versión del sistema operativo), como **/dev/mapper/datos**:

```
/dev/mapper/datos   /datos   ext4   defaults,noatime,nodiratime   1 2
```

Finalmente, se monta la partición cifrada:

```
mount /datos
```

Restaure los datos que respaldó previamente.

```
tar xvf /var/respaldo/datos.tar -C /
```

Restaure los atributos y contextos de SELinux del directorio involucrado.

```
restorecon -R /datos
```

Desmonte la partición:

```
umount /datos
```

Desconecte el dispositivo utilizando el mandato **cryptsetup**, con la opción **luksClose** y el nombre del dispositivo, de acuerdo a como lo vea el planificador de dispositivos:

```
cryptsetup luksClose /dev/mapper/datos
```

Regenere la imagen de disco RAM que utiliza el núcleo del sistema para cargar los controladores necesarios, ejecutando el mandato **dracut** con la opción **-f** para forzar la operación y el archivo del archivo initramfs correspondiente como argumento, la versión del núcleo utilizado, la opción **-a** para añadir módulos de dracut y los nombres de los módulos **dm** y **crypt** como argumentos. El siguiente ejemplo detecta automáticamente el nombre del archivo initramfs y la versión del núcleo que corresponda:

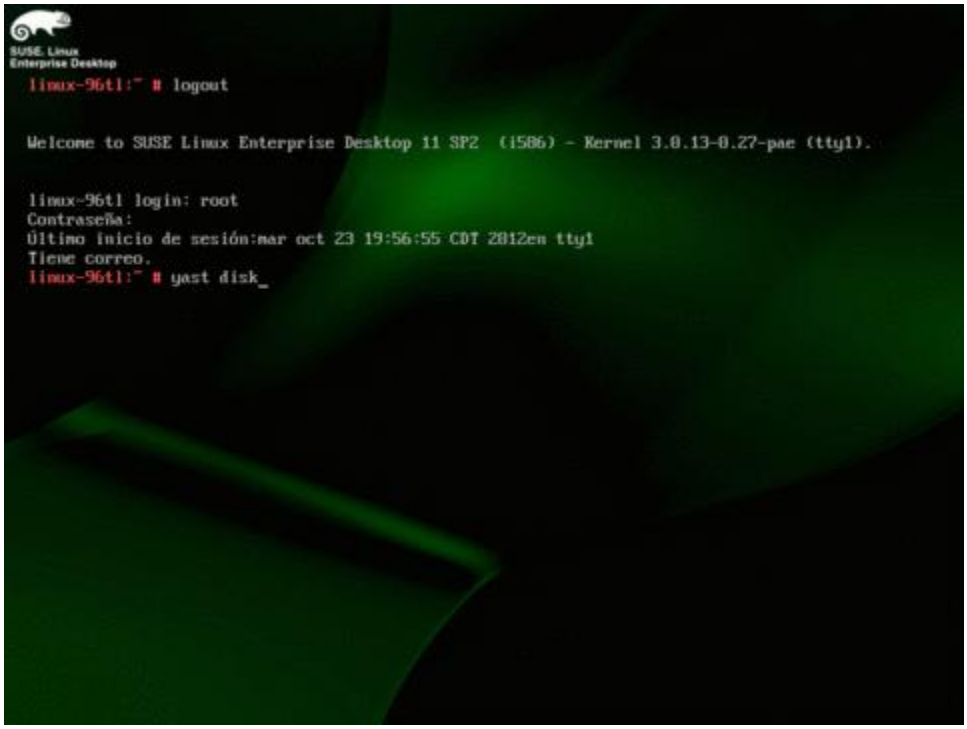
```
dracut -f /boot/initramfs-`uname -r`.img `uname -r` -a dm crypt
```

Reinicie el sistema. En adelante se solicitará la frase de acceso o bien la contraseña, definida durante el procedimiento, para poder iniciar el sistema y así acceder a la partición cifrada.

14.3.2. Cifrado de una partición existente en openSUSE™ y SUSE™ Linux Enterprise.

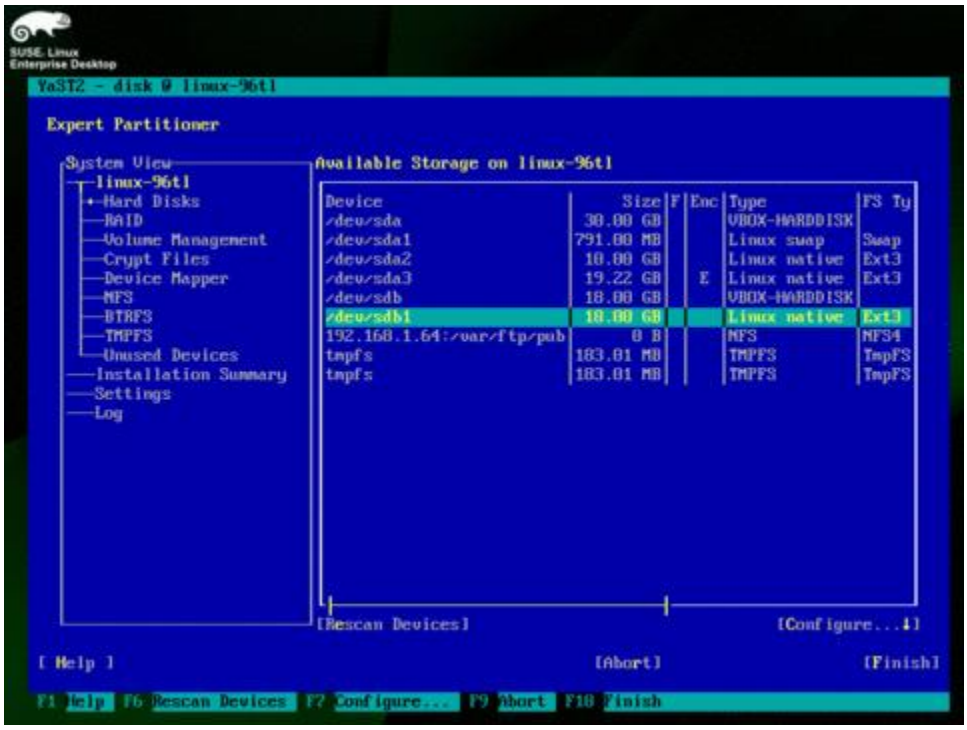
Realice un respaldo de toda la información contenida en la partición que se quiera cifrar. Recuerde que el procedimiento requiere destruir toda la información existente en dicha partición.

Ejecute el mandato **yast** con **disk** como argumento para utilizar el módulo de YaST para gestión de discos y particiones.

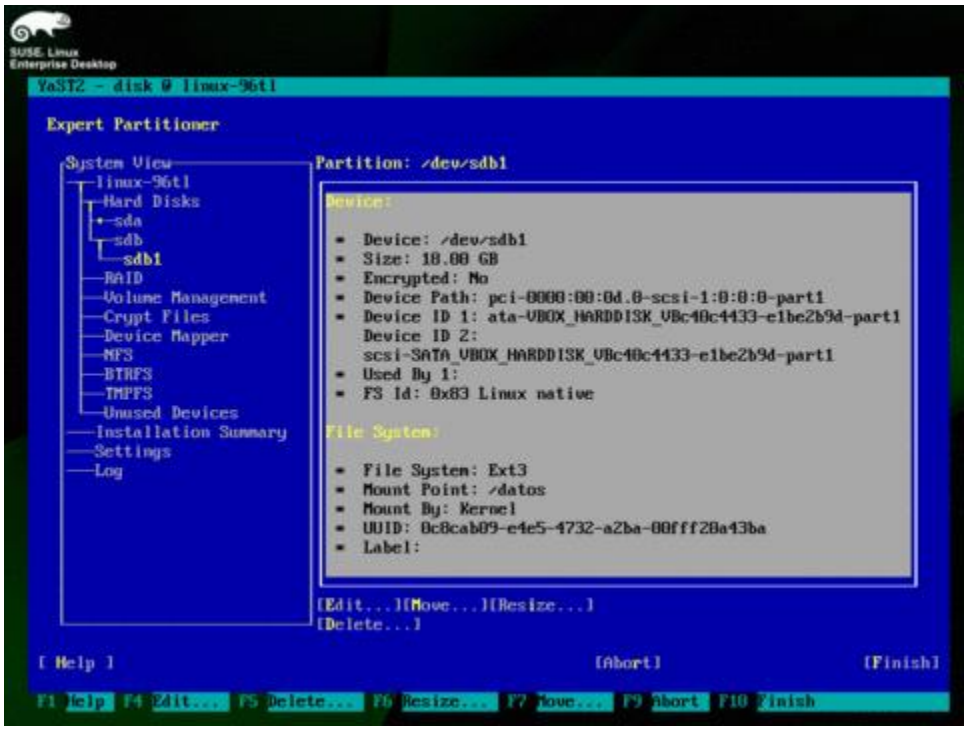


El sistema le advertirá que sólo se debe utilizar este módulo de **YaST** si se entiende perfectamente el concepto de particiones. Responda ***Yes*** o **Si**. Sólo siga las siguientes instrucciones. El ejemplo descrito a continuación considera que se tiene una partición **/dev/sdb1** y que actualmente se utiliza con el directorio /datos como punto de montaje.

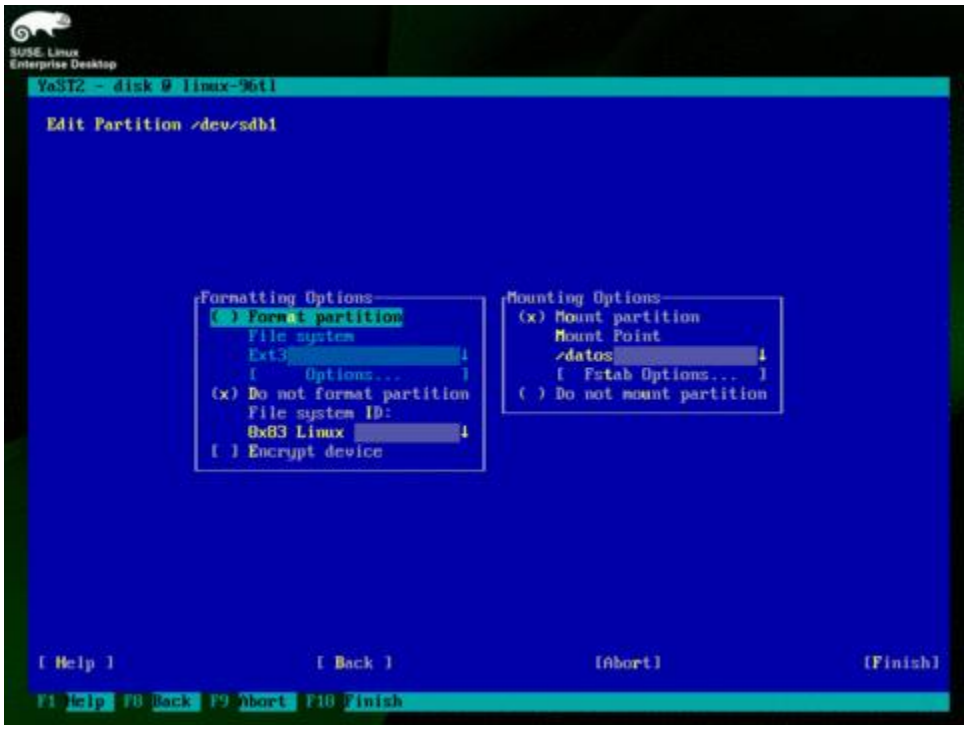
Use la tecla **TAB** hasta seleccionar la partición que requiera cifrar.



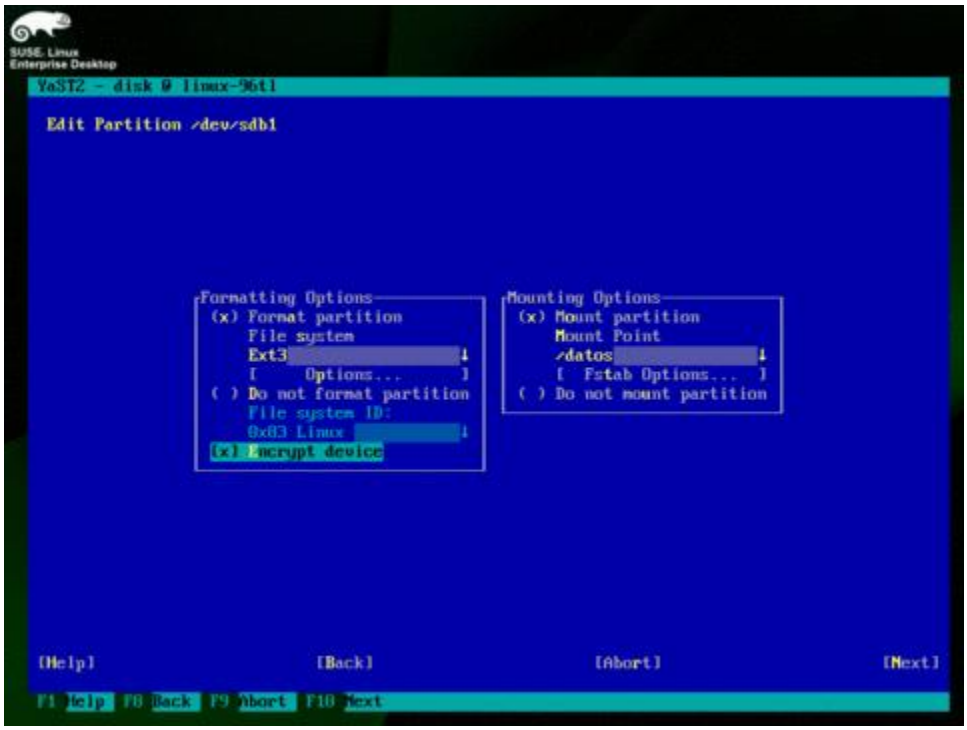
Pulse la tecla **ENTER**. Aparecerá un resumen informativo de la partición seleccionada. Seleccione ***Edit*** o **Editar**.



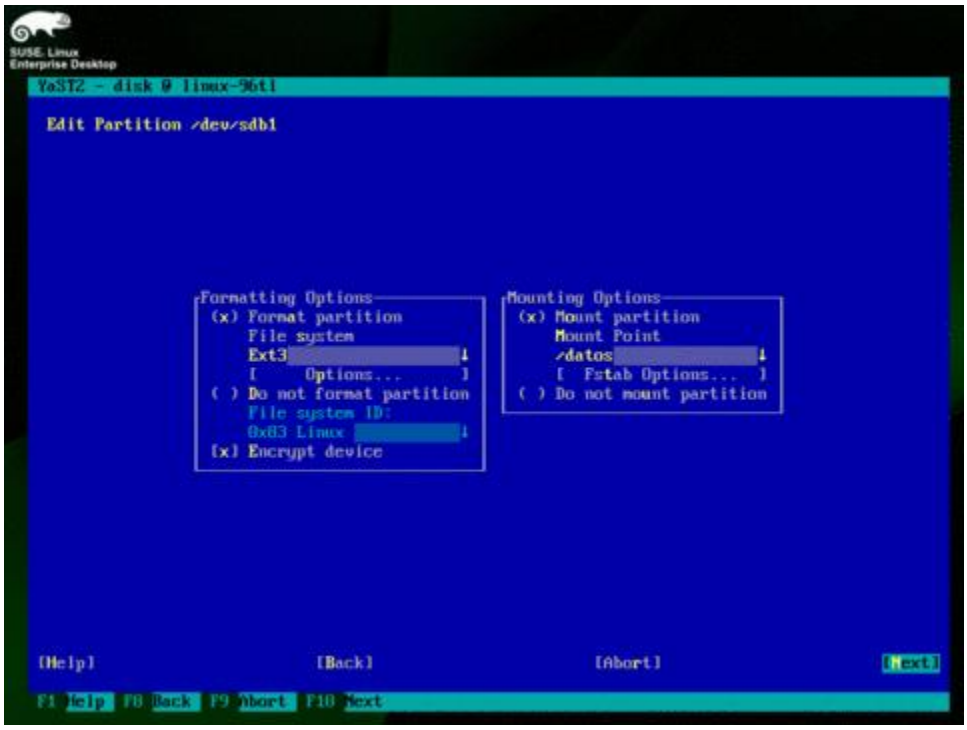
Aparecerán las opciones que se pueden aplicar a la partición.



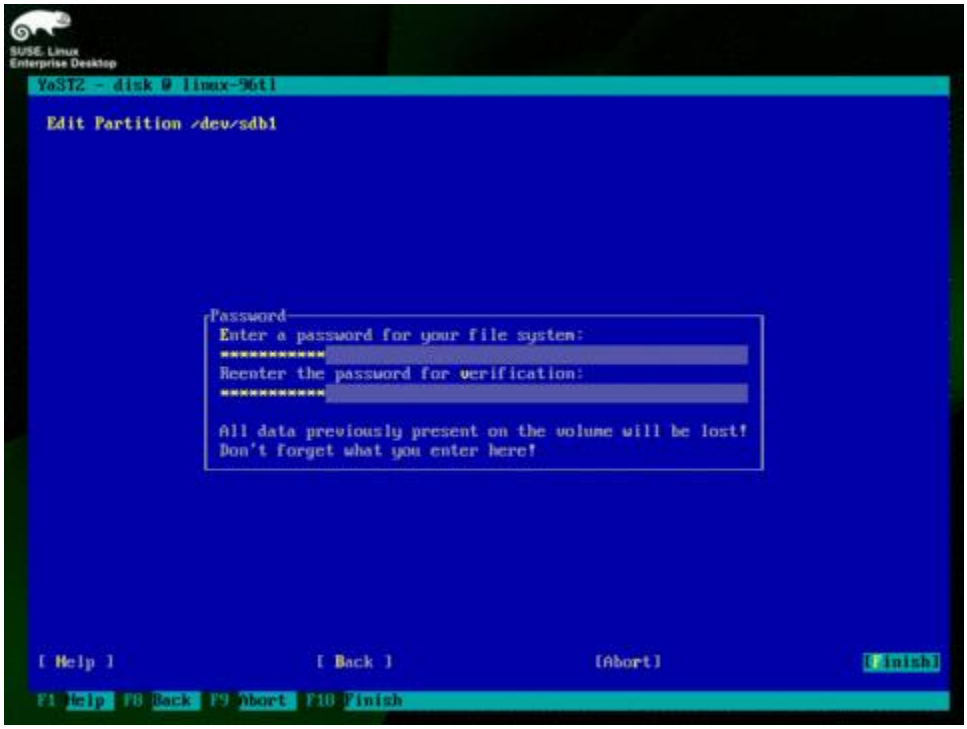
Seleccione las casillas de las opciones ***Format partition*** (o bien Formatear partición) y ***Encrypt partition*** (o bien Cifrar partición).



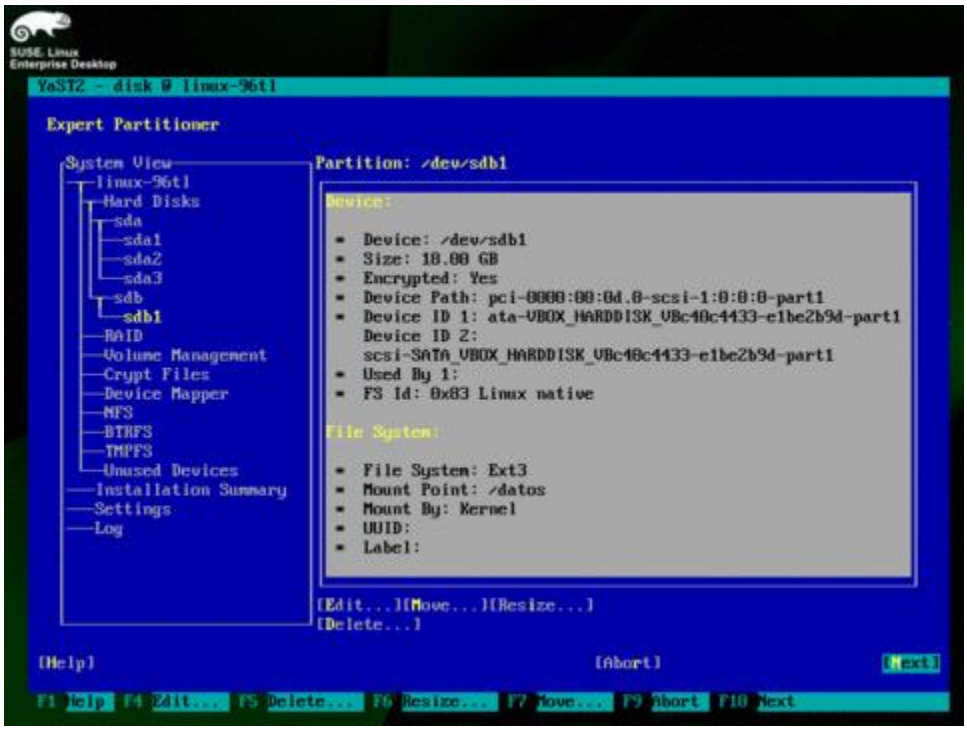
Use la tecla **TAB** hasta seleccionar ***Next*** o Siguiente y pulse la tecla **ENTER**.



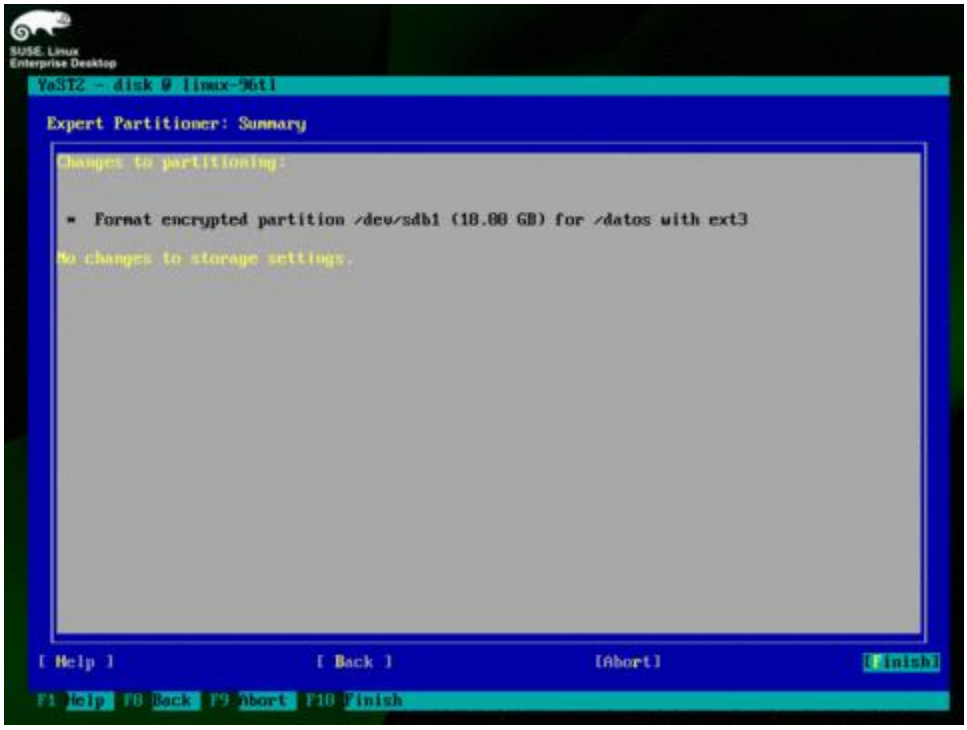
Use la tecla **TAB** y defina una buena contraseña, con confirmación. Recuerde que si olvida o extravía ésta contraseña, la información será irrecuperable. Al terminar, use la tecla **TAB** para seleccionar ***Finish*** o Finalizar y pulse la tecla **ENTER**.



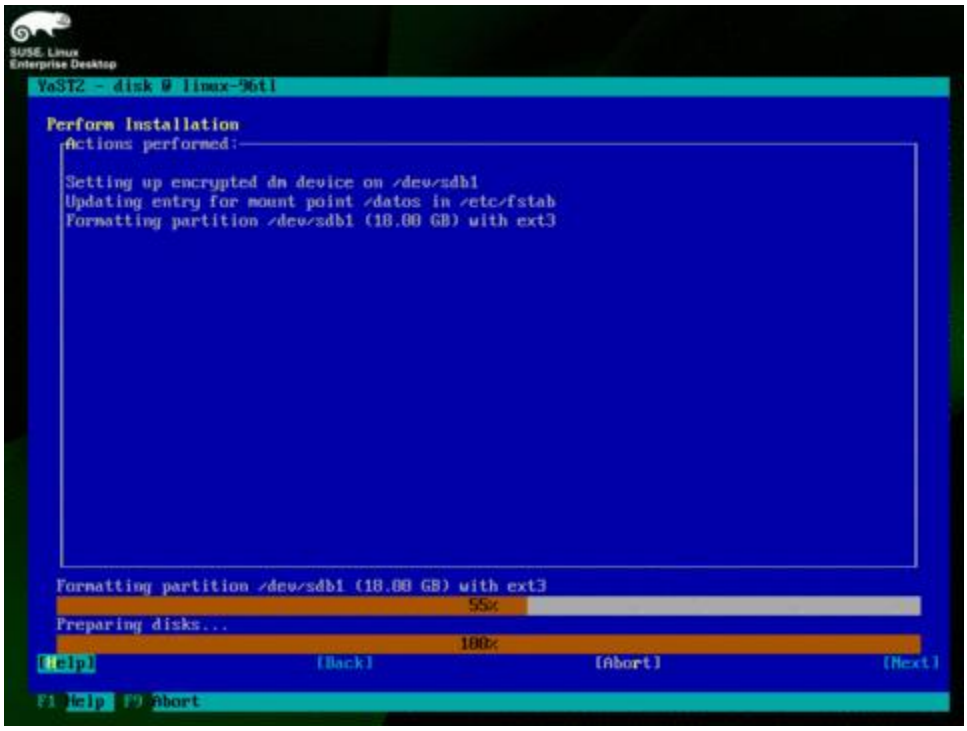
Regresará a la pantalla con el resumen de la partición seleccionada. Use la tecla **TAB** para seleccionar ***Next*** o Siguiente y pulse la tecla **ENTER**.



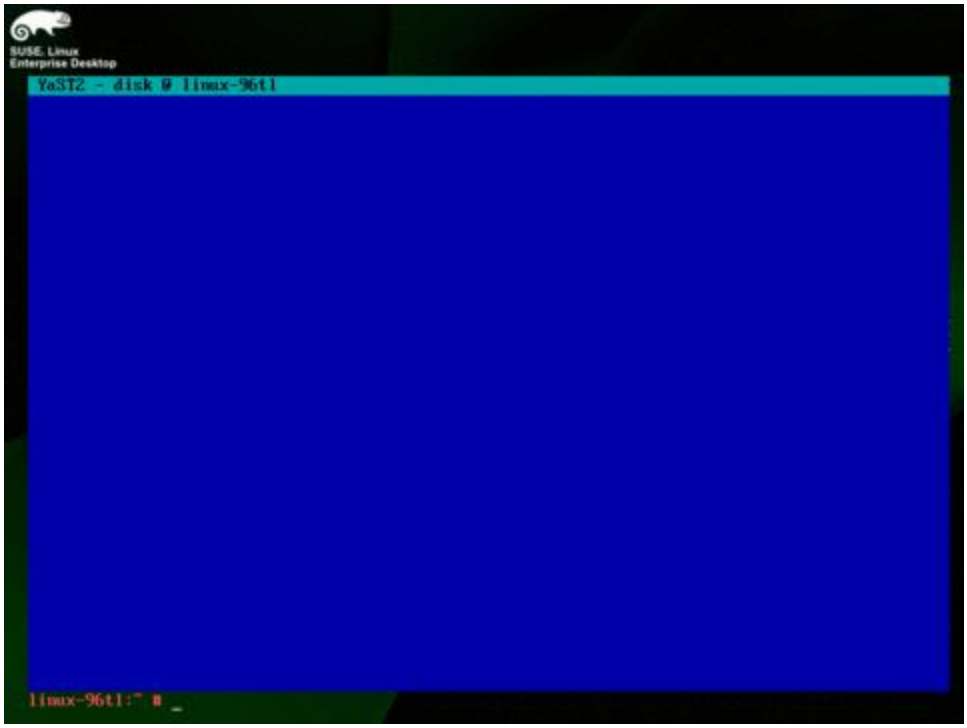
Se mostrará una pantalla con el resumen de los procedimientos que realizará **YaST**. Use la tecla **TAB** para seleccionar ***Finish*** o Finalizar y pulse la tecla **ENTER** o bien sólo pulse la tecla F10.



El sistema realizará todos los procedimientos y cambios necesarios en el sistema indicando el avance de éstos con barras de progreso.



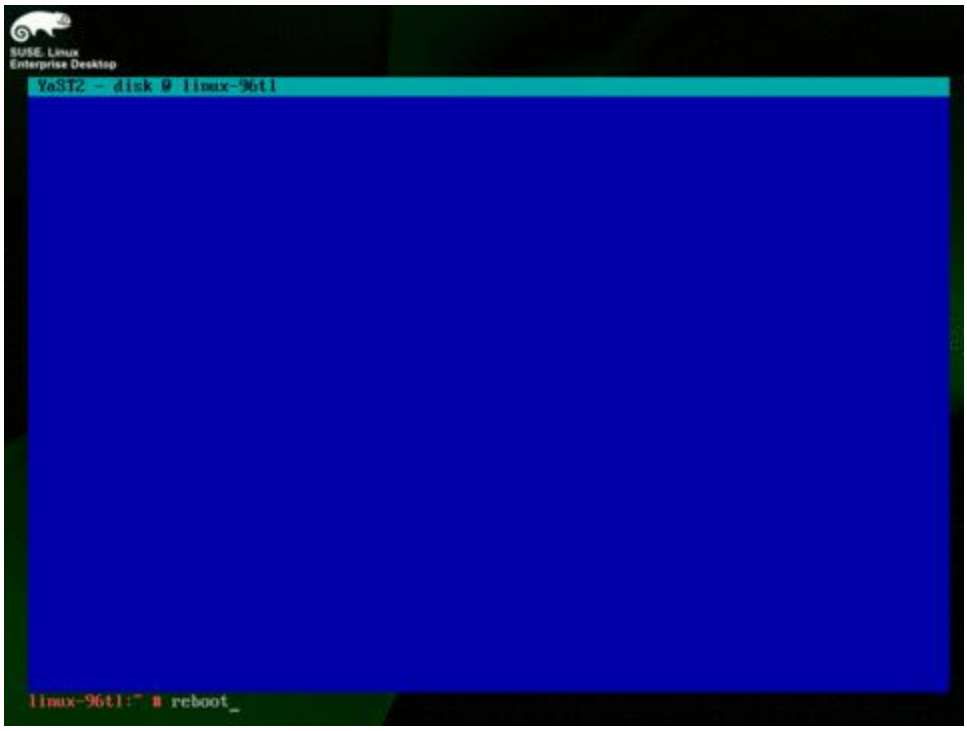
Al terminar, **YaST** finalizará y lo devolverá al intérprete de mandatos.



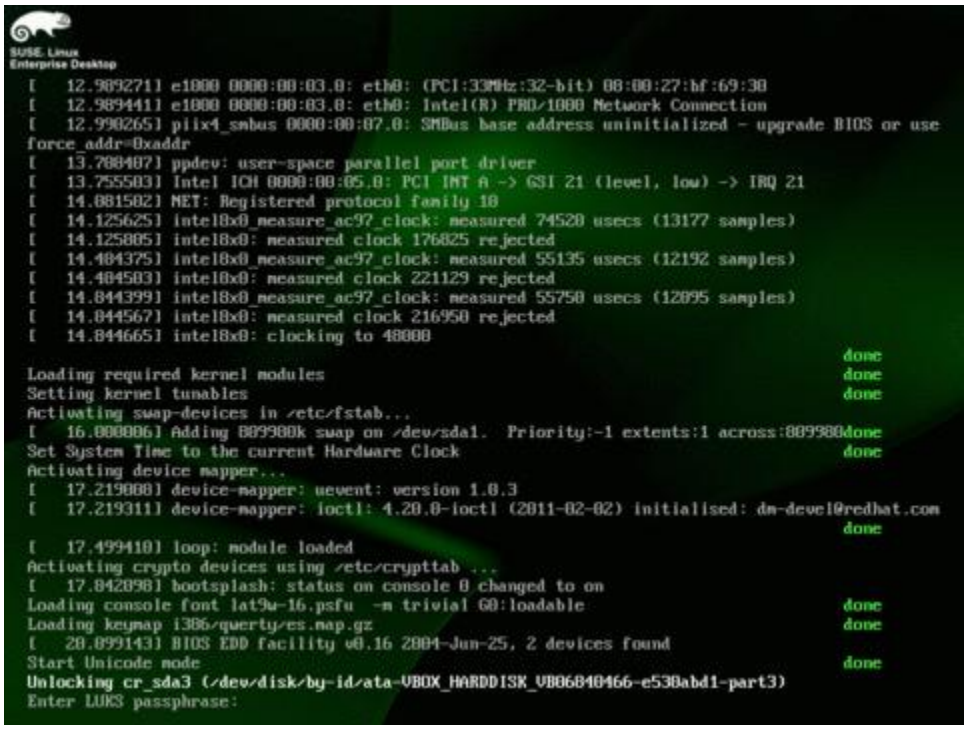
Aunque generalmente YaST se hace cargo automáticamente, regenere la imagen de disco RAM utilizada por el núcleo del sistema para cargar los controladores necesarios, a fin de añadir el soporte necesario para gestor de dispositivos y LUKS. Esto evitará algunos mensajes de error al reiniciar el sistema y garantizará que los controladores necesarios estarán disponibles durante el inicio del sistema. El siguiente ejemplo asume que el dispositivo cifrado corresponde a /dev/mapper/cr_sdb1.

```
mkinitrd -d /dev/mapper/cr_sdb1 -f "dm luks"
```

Reinicie el sistema ejecutando el mandato **reboot**:



Cuando inicie de nuevo el sistema, se hará una pausa en la cual deberá aparecer un diálogo para solicitar la contraseña necesaria para poder desbloquear el dispositivo cifrado.



Tras ingresar la contraseña, el sistema deberá continuar el inicio de manera normal.

Restaure los datos correspondientes a partir del respaldo que debió realizar previamente.

14.3.3. Cifrado de una unidad de almacenamiento externo USB.

El procedimiento asume que ya se ha realizado un respaldo de los datos de la unidad de almacenamiento externo USB, pues el procedimiento implica la destrucción de los datos existentes en ésta.

Conecte el dispositivo USB y utilice el mandato **dmesg** del siguiente modo para determinar que partición que corresponda al dispositivo.

```
dmesg |grep sd
```

Lo anterior debe devolver algo similar a lo siguiente.

```
[ 1368.902764] sd 6:0:0:0: Attached scsi generic sg2 type 0
[ 1368.904999] sd 6:0:0:0: [sdb] 4122624 512-byte logical blocks: (2.11 GB/1.96 GiB)
[ 1368.906562] sd 6:0:0:0: [sdb] Write Protect is off
[ 1368.906572] sd 6:0:0:0: [sdb] Mode Sense: 03 00 00 00
[ 1368.907176] sd 6:0:0:0: [sdb] No Caching mode page present
[ 1368.907183] sd 6:0:0:0: [sdb] Assuming drive cache: write through
[ 1368.910295] sd 6:0:0:0: [sdb] No Caching mode page present
[ 1368.910303] sd 6:0:0:0: [sdb] Assuming drive cache: write through
[ 1369.174678]  sdb: sdb1
[ 1369.182877] sd 6:0:0:0: [sdb] No Caching mode page present
[ 1369.182886] sd 6:0:0:0: [sdb] Assuming drive cache: write through
[ 1369.182892] sd 6:0:0:0: [sdb] Attached SCSI removable disk
```

Si el sistema monta automáticamente la unidad de almacenamiento externo, determine el punto de montaje y dispositivo asignado con el mandato **df**.

```
df
```

Si el sistema monta automáticamente la unidad de almacenamiento externo y asumiendo que el sistema asignó el directorio **/media/MI-USB** como punto de montaje, desmonte la unidad:

```
umount /media/MI-USB
```

Asumiendo que la partición de la unidad de almacenamiento externo corresponde al dispositivo **/dev/sdb1**, utilice el mandato **cryptsetup**, con las opciones **--verbose** (para obtener una salida más descriptiva en caso de problemas), **--verify-passphase** (para asignar una frase de acceso o bien una contraseña), **luksFormat** para dar formato en LUKS y el nombre del dispositivo.

```
cryptsetup --verbose --verify-passphrase luksFormat /dev/sdb1
```

Lo anterior requerirá responder explícitamente con **YES**, en mayúsculas, que se desea proceder y que se está consciente que se perderán todos los datos actuales de la partición. A continuación, se pulsa la tecla **ENTER** y se ingresa la nueva frase o bien la nueva contraseña, que se pretenda asignar.

Una vez realizado lo anterior, para poder hacer uso de la nueva partición cifrada en la unidad de almacenamiento externo USB, se utiliza el mandato **cryptsetup** con la opción **luksOpen**, indicando el dispositivo que corresponde a la partición que se acaba de cifrar y el nombre que se quiera asignar a ésta en el planificador de dispositivos (*device mapper*).

```
cryptsetup luksOpen /dev/sdb1 MI-USB
```

Lo anterior crea un nuevo dispositivo denominado **/dev/mapper/MI-USB**.

Para que el sistema operativo pueda utilizarlo, este nuevo dispositivo requiere un formato que pueda ser utilizado en cualquier sistema operativo. En el siguiente ejemplo se da formato en FAT32 a **/dev/mapper/MI-USB**:

```
mkfs.vfat /dev/mapper/MI-USB
```

Monte la partición de la unidad de almacenamiento externo en /media/MI-USB:

```
mkdir /media/MI-USB
mount /dev/mapper/MI-USB /media/MI-USB
```

Restaure o copie los datos que requiera utilizar en esta unidad de almacenamiento.

Desmonte la unidad.

```
umount /media/MI-USB
```

Desconecte el dispositivo cifrado:

```
cryptsetup luksClose /dev/mapper/MI-USB
```

Para utilizar en lo sucesivo la unidad de almacenamiento externo USB desde modo terminal, sin escritorio activo, se sigue el siguiente procedimiento:

```
mkdir /mnt/mi-usb
cryptsetup luksOpen /dev/sdb1 mi-usb
mount /dev/mapper/mi-usb /mnt/mi-usb
```

Para utilizar la unidad de almacenamiento externo USB cifrada con LUKS desde el escritorio de GNOME o KDE, se inserta ésta en cualquier puerto USB, dejando que el administrador de archivos se encargue de gestionar lo necesario y mostrar el dialogo para ingresar la clave o frase de acceso necesaria.

Para utilizar la unidad de almacenamiento externo USB cifrada con LUKS desde el escritorio Windows, sólo hay que instalar **FreeOTFE**, insertar la unidad a cualquier puerto USB, permitiendo que **FreeOTFE** se encargue de gestionar lo necesario y mostrar el dialogo para ingresar la clave o frase de acceso necesaria. Sin **FreeOTFE**, Windows solo vería una unidad de almacenamiento externo USB sin formato, mostrando un dialogo para dar formato a ésta.

15. Configuración y uso de sudo

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

15.1. Introducción.

15.1.1. Historia.

Sudo fue inicialmente concebido en 1980 por Bob Coggeshall y Cliff Spencer del Departamento de Ciencia Computacional en **SUNY** (**S**tate **U**niversity of **N**ew **Y**ork o Universidad Estatal de Nueva York), en Buffalo.

En 1985 se publicó una versión mejorada acreditada a Phil Betchel, Cliff Spencer, Gretchen Phillips, John LoVerso y Don Gworek en el grupo de noticias *net.sources*. Garth Snyder publicó otra versión mejorada en el verano de 1986 y durante los siguientes cinco años fue mantenido con la colaboración de muchas personas, incluyendo Bob Coggeshall, Bob Manchek y Trent Hein.

Dave Hieb y Jeff Nieusma escribieron en 1991 una versión mejorada del formato para el archivo **/etc/sudoers**, bajo contrato con la firma consultora The Root Group, versión que posteriormente fue publicada bajo los términos de la Licencia Pública General de GNU (GNU/GPL).

Desde 1996 el proyecto es mantenido activamente por Todd Miller, con la colaboración de Chris Jepeway y Aaron Spangler y actualmente se distribuye bajo los términos de una licencia tipo BSD.

15.1.2. Acerca de sudo.

Sudo (**Su**peruser **Do**) es una herramienta de sistema que permite a los usuarios realizar la ejecución de mandatos como super-usuario u otro usuario de acuerdo a como se especifique en el archivo **/etc/sudoers**, donde se determina quien está autorizado. Los números de identidad de usuario y de grupo (UID y GID) reales y efectivas se establecen para igualar a aquellas del usuario objetivo como esté especificado en el archivo **/etc/passwd**.

Por seguridad, de modo predeterminado el mandato **sudo** requiere que los usuarios regulares autorizados se autentiquen así mismos, es decir con su propia clave de acceso, **nunca con la contraseña de root**. También es obligatorio el acceso desde una terminal (**TTY**) para poder ejecutar el mandato **sudo** y si un usuario sin autorización lo ejecuta, se registrará la actividad en la bitácora de sistema (a través de **syslogd**) y se enviará un mensaje de correo electrónico al administrador del sistema (root).

El manual de información del formato del archivo **/etc/sudoers** se puede consultar ejecutando lo siguiente:

```
man 5 sudoers
```

El manual de información del mandato **sudo** se puede consultar ejecutando lo siguiente:

```
man 8 sudo
```

El manual de información del mandato **visudo** se puede consultar ejecutando lo siguiente:

```
man 8 visudo
```

15.2. Equipamiento lógico necesario.

15.2.1. Instalación en CentOS, Fedora y Red Hat™ Enterprise Linux.

Sudo viene incluido junto con la instalación estándar de estos sistemas operativos. De ser necesario, ejecute lo siguiente para instalar el paquete **sudo**:

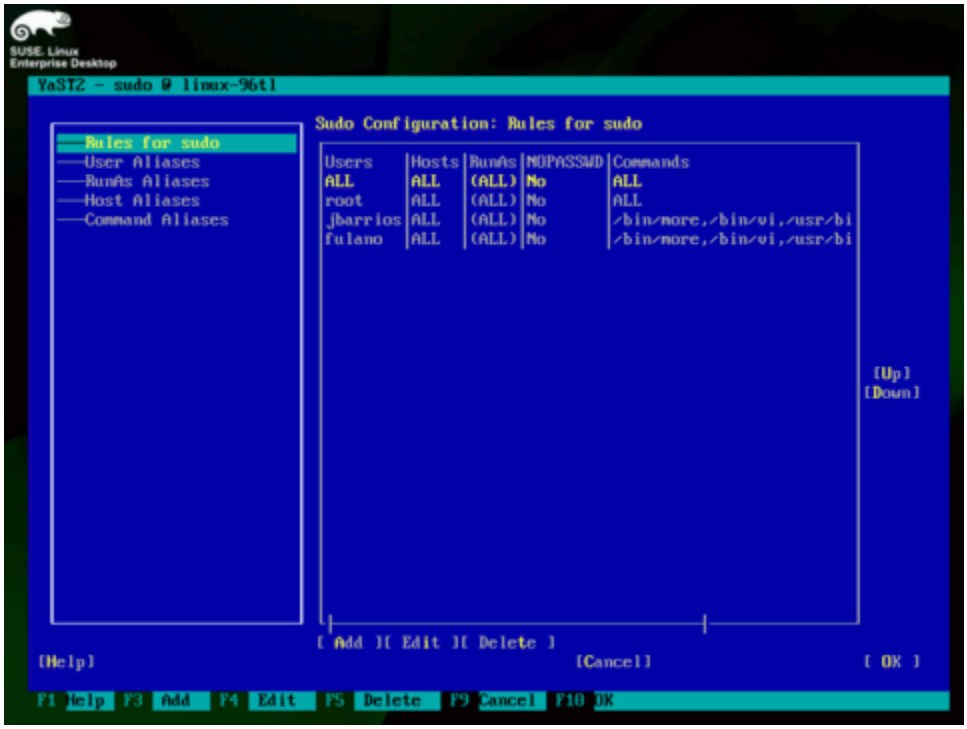
```
yum -y install sudo
```

15.2.2. Instalación en openSUSE y SUSE Linux Enterprise.

Sudo viene incluido junto con la instalación estándar de estos sistemas operativos. De ser necesario, ejecute lo siguiente para instalar el paquete **sudo**:

```
yast -i sudo
```

Existe un módulo de sudo para YaST, pero tiene un soporte muy limitado en cuanto a funciones. Permite editar usuarios, crear y administrar las listas de control de acceso, pero carece de soporte para funciones como NOEXEC en las reglas de control de acceso y negaciones dentro de las listas de control de acceso.



Módulo sudo de YaST, en modo texto.

Si decide utilizar el módulo sudo de YaST, ejecute lo siguiente:

```
yast -i yast2-sudo
```

15.3. Archivo /etc/sudoers

El archivo **/etc/sudoers** se edita con el mandato **visudo**, herramienta que a través de vi permite realizar cambios y verificar sintaxis y errores. Si se trata de modificar directamente **/etc/sudoers**, éste tiene permisos de sólo lectura.

La sintaxis básica de una lista sería:

```
XXXX_Alias NOMBRELISTA = elemento1, elemento2, elemento3
```

La sintaxis básica de una regla sería:

```
[usuario, %grupo, NOMBRELISTA] [anfitrión] = (id de usuario a usar) mandatos
```

Se pueden definir Aliases y reglas. Los aliases permiten definir listas de mandatos, listas de usuarios, listas de anfitriones o bien listas de identidades de usuarios para ejecutar mandatos.

15.3.1. Cmnd_Alias.

Se utiliza para definir listas de mandatos a utilizar con sudo y/o excluir su ejecución con sudo. Ejemplo:

```
Cmnd_Alias MANDATOS4 = /sbin/service httpd reload, \
        /usr/bin/vim /etc/httpd/conf.d/variables.conf, \
        /usr/bin/vim /etc/php.ini
```

Lo anterior define una lista de mandatos que podrían utilizarse para hacer que el servicio **httpd** vuelva a leer su configuración, modificar los archivo **/etc/httpd/conf.d/variables.conf** y **/etc/php.ini**.

```
fulano ALL = MANDATOS4
```

Lo anterior define que el usuario fulano puede utilizar los mandatos de la lista MANDATOS4 desde cualquier anfitrión.

También se pueden definir mandatos prohibidos junto con mandatos permitidos. Por ejemplo:

```
Cmnd_alias ALTACUENTAS = /usr/sbin/useradd, /usr/bin/passwd *, \
                            !/usr/bin/passwd root

fulano  ALL = (ALL) ALTACUENTAS
```

Lo anterior define que fulano puede utilizar el mandato **useradd** con cualquier opción y argumentos y el mandato passwd con cualquier argumento, pero tendrá prohibido utilizar el mandato **passwd** con *root* como argumento, es decir tendrá prohibido cambiar la contraseña de root.

En el siguiente ejemplo, el usuario fulano podría utilizar virtualmente cualquier mandato del sistema, excepto los mandato **passwd** con *root* como argumento y los mandatos **bash, userdel, usermod y su.**

```
Cmnd_alias PROHIBIDOS = !/bin/su, !/bin/bash, !/usr/sbin/usermod, \
    !/usr/sbin/userdel, !/usr/bin/passwd root

fulano  ALL = (ALL) ALL, PROHIBIDOS
```

15.3.2. User_Alias.

Se utiliza para definir listas de usuarios y/o grupos que podrán utilizar sudo y/o aquellos que tendrán prohibido utilizarlo. Ejemplo:

```
User_Alias WEBADMINS = fulano, mengano, zutano
```

Lo anterior define una lista denominada **WEBADMINS**, integrada por los usuarios fulano, mengano y zutano.

```
WEBADMINS ALL = /usr/bin/vim
```

La regla anterior define que los usuarios que conforman la lista **WEBADMINS** pueden utilizar el mandato vim desde cualquier anfitrión.

También es posible definir grupos a los cuales pertenecen los usuarios del sistema. Ejemplo:

```
User_Alias ADMINS = %wheel, !pepe
```

Lo anterior define una lista denominada **ADMINS**, integrada por los usuarios que pertenezcan al grupo de sistema denominado **wheel**, excluyendo el usuario denominado **pepe**.

```
ADMINS ALL = /usr/bin/vim
```

La regla anterior define que los usuarios que conforman la lista **ADMINS**, es decir todos los miembros del grupo de sistena denominado **wheel**, excepto el usuario denominado **pepe**, pueden utilizar el mandato vim desde cualquier anfitrión.

15.3.3. Host_Alias.

Se utiliza para definir listas de anfitriones desde los cuales se tendrá permitido utilizar sudo o bien desde los cuales se tendrá prohibido utilizarlo. Ejemplo:

```
Host_Alias WEBHOSTS = 192.168.70.25, \
            192.168.70.26, \
            192.168.70.23
```

Lo anterior define que la lista **WEBHOSTS** está integrada por las 3 direcciones IP listadas anteriormente. Si además se añade la siguiente regla:

```
WEBADMINS WEBHOSTS =  ADMINHTTPD
```

Lo anterior define que los usuarios de la lista **WEBADMINS** pueden utilizar los mandatos listados en **ADMINHTTPD** solamente si están conectados desde las direcciones IP listadas en **WEBHOSTS**.

15.3.4. Runas_Alias.

Se utiliza para definir listas de identidades permitias para utilizar sudo o bien aquellas que estarán prohibido utilizar. Ejemplo:

Si por ejemplo se quisiera que los usuarios de la lista **WEBADMINS** pudieran además utilizar los mandatos ls, rm, chmod, cp, mv, mkdir, touch y vim como el usuarios juan, pedro y hugo, se requiere definir una lista para estos mandatos y otra para los aliases de usuarios alternos y la regla correspondiente.

```
User_Alias WEBADMINS = fulano, mengano, zutano

Runas_Alias WEBUSERS1 = juan, pedro, hugo

Cmnd_Alias MANDATOS1 = /bin/ls, /bin/rm, /bin/chmod, \
        /bin/cp, /bin/mv, /bin/mkdir, /bin/touch, \
        /usr/bin/passwd [A-z]*, !/usr/bin/passwd root

WEBADMINS WEBHOSTS = (WEBUSERS1) MANDATOS3
```

Lo anterior permite a los usuarios definidos en **WEBADMINS** (es decir fulano, mengano y zutano), utilizar los mandatos definidos en **MANDATOS1** (es decir podrán utilizar los mandatos ls, rm, chmod, cp, mv, mkdir, touch, vim y passwd, pero para el este último estará prohibido cambiar la contraseña de root), identificándose como los usuarios definidos en la lista **WEBUSERS1** (juan, pedro y hugo), sólo si el mandato **sudo** se ejecuta desde los anfitriones con las direcciones IP listadas en **WEBHOSTS** (192.168.70.25, 192.168.70.26, 192.168.70.23).

Al momento de establecer las reglas, es posible especificar el permiso de ejecución de ciertos mandatos con uno o más usuarios y el de otros mandatos con otros usuarios distintos.

```
User_Alias WEBADMINS = fulano, mengano, zutano

Runas_Alias WEBUSERS1 = juan, pedro, hugo

Runas_Alias WEBUSERS2 = mario, beto, paco

Cmnd_Alias MANDATOS1 = /bin/ls, /bin/rm, /bin/chmod, \
        /bin/cp, /bin/mv, /bin/mkdir, /bin/touch, \
        /usr/bin/passwd [A-z]*, !/usr/bin/passwd root

Cmnd_Alias MANDATOS2 = /usr/bin/vim, /bin/cat, \
        /usr/bin/less

WEBADMINS WEBHOSTS = (WEBUSERS1) MANDATOS1 (WEBUSERS2) MANDATOS1
```

Lo anterior establece que los miembros de la lista **WEBADMINS** (fulano, mengano y zutano) pueden ejecutar desde lo anfitriones definidos en **WEBHOSTS** los mandatos definidos en la lista MANDATOS1, pero sólo adoptando las identidades de juan, pedro y hugo y los mandatos definidos en la lista MANDATOS2, pero sólo pueden ser ejecutados adoptando las identidades de mario, beto y paco.

Basado sobre el ejemplo anterior, estaría permitido ejecutar algo como lo siguiente:

```
sudo -u juan mkdir /home/juan/public_html/images
```

Pero estaría prohibido ejecutar lo siguiente, porque sólo se permite usar el mandato /bin/cp con las identidades juan, pedro y hugo:

```
sudo -u mario cp -r /home/mario/public_html/images2/* \
    /home/mario/public_html/images2/
```

15.4. Candados de seguridad.

Algunos mandatos, como el caso de los mandatos **less**, **vi**, **vim** y **more**, permiten ejecutar otros mandatos en el intérprete de mandatos (lo que se conoce como *Shell Escape* o escape al intérprete de mandatos). En estos casos se puede utilizar **NOEXEC** para impedir que algunos mandatos permitan la ejecución con privilegios de otros mandatos. Ejemplo:

```
fulano ALL = (ALL) ALL \
    NOEXEC: /bin/vi, /usr/bin/less, /usr/bin/vim, /bin/more
```

Lo anterior permitiría al usuario fulano poder editar o visualizar con privilegios cualquier archivo del sistema utilizando el mandato **vim** y el mandato **more**, pero deshabilita la posibilidad de poder ejecutar otros mandatos con privilegios desde el escape al intérprete de mandatos de **vim**.

El mandato **sudo** incluye varios candados de seguridad (predeterminados) que impiden se puedan realizar tareas peligrosas, como redirigir la salida estándar de un mandato (**STDOUT**) hacia archivos fuera del directorio de inicio del usuario utilizado.

Si se define en el archivo **/etc/sudoers** que un usuario puede utilizar con privilegios el mandato **/usr/bin/vim**, es decir algo como lo siguiente:

```
fulano ALL = (ALL) /bin/echo, \
    NOEXEC: /bin/vi, /usr/bin/vim, /bin/more, /usr/bin/less
```

El mandato **sudo** permitirá que el usuario regular definido pueda ejecutar el mandato **/usr/bin/vim** de los siguientes modos:

```
sudo /usr/bin/vim
sudo vim
```

Pero se impedirá ejecutar el mandato **vim** del siguiente modo:

```
cd /usr/bin
sudo ./vim
```

Si, por ejemplo se define en el archivo **/etc/sudoers** que un usuario puede utilizar con privilegios el mandato **/bin/echo**, es decir algo como lo siguiente:

```
fulano ALL = (ALL) /bin/echo, \
    NOEXEC: /bin/vi, /usr/bin/vim, /bin/more, /usr/bin/less
```

El usuario sólo podrá utilizar el mandato **echo** de los siguientes modos, asumiendo que se trata del usuario fulano:

```
sudo /bin/echo "Hola" > /home/fulano/prueba.txt
sudo echo "Hola" > /home/fulano/prueba.txt
```

Sin embargo, el mandato **sudo** impedirá a los usuarios regulares redirigir la salida estándar hacia archivos fuera de sus propios directorios de inicio, como por ejemplo al ejecutar algo como lo siguiente:

```
sudo echo "Hola" > /etc/prueba.txt
```

Para poder realizar la operación anterior, se tendría que ejecutar:

```
sudo bash -c "echo 'Hola' > /etc/prueba.txt"
```

Para impedir lo anterior, habría que prohibir en el archivo **/etc/sudoers** el uso del mandato /bin/bash, como se muestra en el siguiente ejemplo:

```
fulano ALL = (ALL) ALL, !/bin/su, !/bin/bash \
    !/usr/bin/sudo, !/usr/bin/visudo, \
    NOEXEC: /bin/vi, /usr/bin/vim, /bin/more, /usr/bin/less
```

El mandato **sudo** permitirá realizar una tarea con privilegios sobre cualquier archivo dentro de cualquier directorio, aún si el usuario regular carece de permisos de acceso para ingresar a dicho directorio, siempre y cuando especifique **la ruta exacta** de dicho archivo. Ejemplo:

```
sudo chown named /var/named/dominio.zone
```

Cuando el usuario regular carece de permisos de acceso a un directorio o sub-directorio en particular, el mandato **sudo** siempre impedirá ejecutar algo como lo siguiente:

```
sudo chown named /var/named/*.zone
```

15.5. Lo más recomendado.

Si se va a permitir la ejecución de todos los mandatos del sistema utilizando el mandato **sudo**, como mínimo prohíba el uso de **/bin/bash**, **/bin/su**, **/usr/bin/sudo** (para prevenir se pueda ejecutar «*sudo sudo mandato*»), **/usr/bin/passwd root** y **/usr/sbin/visudo** y restrinja el uso de mandatos que permitan escape al intérprete de mandatos, como serían **/usr/bin/less**, **/bin/more**, **/bin/vi** y **/usr/bin/vim**. Ejemplo:

```
fulano ALL = (ALL) ALL, \
    !/bin/bash, !/bin/su, !/usr/sbin/visudo, !/usr/bin/passwd root, \
    !/usr/bin/sudo, \
    NOEXEC: /bin/more, /bin/vi, /usr/bin/less, /usr/bin/vim
```

De ser posible, evite definir **ALL** (todos los mandatos) y sólo permita la ejecución de mandatos específicos. Puede definir todos los que quiera. Ejemplo:

```
fulano ALL = (ALL) /bin/cat, /bin/chgrp, /sbin/chkconfig, /bin/chmod, \
    /bin/chown, /sbin/depmod, /usr/sbin/edquota, /usr/sbin/groupadd, \
    /usr/bin/htpasswd, /sbin/ip, /usr/bin/openssl, /sbin/service, \
    /usr/bin/tail, /usr/sbin/useradd, /usr/bin/passwd [A-z]*, \
    !/usr/bin/passwd root, \
    NOEXEC: /bin/more, /bin/vi, /usr/bin/less, /usr/bin/vim
```

Evite utilizar nombres de usuario y, sobre todo, contraseñas predecibles o fáciles de adivinar.

15.5.1. Lo menos recomendado.

Si se quiere permitir a un usuario ejecutar con el mandato **sudo** prácticamente **lo que sea**, desde cualquier anfitrión, utilizando cualquier identidad de usuario del sistema y **requiriendo ingresar la contraseña correspondiente** al menos cada 5 minutos, se puede definir:

```
fulano ALL = (ALL) ALL
```

La configuración predeterminada en distribuciones basadas sobre Ubuntu Linux utiliza lo siguiente:

```
%wheel ALL = (ALL) ALL
```

Con lo anterior, sólo los usuarios miembros al grupo de sistema denominado **wheel** podrán hacer uso del mandato **sudo**. Se recomienda cambiar esta configuración para hacerla un poco más restrictiva, como la que se muestra en los ejemplos citados unos párrafos arriba.

Si se quiere permitir a un usuario ejecutar con el mandato **sudo** prácticamente **lo que sea**, desde cualquier anfitrión, utilizando cualquier identidad de usuario del sistema y **sin necesidad de autenticar**, se puede definir algo como lo siguiente:

```
fulano ALL = (ALL) NOPASSWD: ALL
```

Dentro de lo posible, evite utilizar esta última configuración.

15.6. Uso del mandato sudo.

Ejecutando el mandato **sudo** con la opción **-l** (minúscula) como usuario regular se muestran las opciones de variables de entorno permitidas y la lista de mandatos permitidos y prohibidos.

```
sudo -l
```

La salida puede ser algo similar a lo siguiente:

```
Matching Defaults entries for jbarrios on this host:
    requiretty, env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE
    INPUTRC KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR USERNAME
    LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION
    LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY LC_NAME
    LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE
    LINGUAS _XKB_CHARSET XAUTHORITY",
    secure_path=/sbin:/bin:/usr/sbin:/usr/bin

User fulano may run the following commands on this host:
        (ALL) NOPASSWD: ALL, (ALL) !/sbin/fdisk, (ALL) NOEXEC: /usr/bin/vim,
    (ALL) /bin/more
```

Para listar los privilegios de un usuario en particular, se ejecuta como root el mandato **sudo** con la opción **-l** (minúscula), la opción **-U** (mayúscula) y el nombre del usuario a consultar. Ejemplo:

```
sudo -l -U fulano
```

Ejecutando el mandato **sudo** con la opción **-L** (mayúscula) se muestran todas las opciones soportadas en el archivo **/etc/sudores**.

```
sudo -L
```

La salida, **que es muy extensa**, puede incluir algo similar a lo siguiente:

```
Available options in a sudoers ``Defaults'' line:

syslog: Syslog facility if syslog is being used for logging
syslog_goodpri: Syslog priority to use when user authenticates
successfully
syslog_badpri: Syslog priority to use when user authenticates
unsuccessfully
long_otp_prompt: Put OTP prompt on its own line
ignore_dot: Ignore '.' in $PATH
mail_always: Always send mail when sudo is run
...
pwfeedback: Provide visual feedback at the password prompt when there
is user input
fast_glob: Use faster globbing that is less accurate but does not
access the filesystem
umask_override: The umask specified in sudoers will override the
user's, even if it is more permissive
log_input: Log user's input for the command being run
log_output: Log the output of the command being run
compress_io: Compress I/O logs using zlib
use_pty: Always run commands in a pseudo-tty
```

Para ejecutar un mandato con sudo, se utiliza la siguiente sintaxis.

```
sudo -[opciones] mandato
```

Ejemplo:

```
sudo service cups restart
```

Si se omite especificar opciones, se asume que el usuario y grupo utilizados para la identidad serán root.

Para especificar que una operación se ejecute como un usuario en particular, se ejecuta el mandato **sudo** con la opción **-u** (minúscula) seguida del nombre del usuario a utilizar y el mandato correspondiente como argumento. Ejemplo:

```
sudo -u zutano vim /home/zutano/datos.txt
```

Para especificar que una operación se ejecute como un miembro de un grupo en particular, se ejecuta el mandato **sudo** con la opción **-g** seguida del nombre del grupo a utilizar y el mandato correspondiente como argumento. Ejemplo:

```
sudo -g lp lpadmin -x EPL-5900
```

Para especificar que una operación se realice en segundo plano, se ejecuta el mandato **sudo** con la opción **-b** y el mandato correspondiente como argumento. Ejemplo:

```
sudo -b tar cpf /var/respaldos/respaldo-etc.tar /etc
```

Una vez que el usuario se ha autenticado, el usuario podrá utilizar nuevamente sudo sin necesidad de volver a autenticarse durante 5 minutos, salvo que se especifique lo contrario en el archivo **/etc/sudoers**. Si un usuario regular ejecuta el mandato **sudo** con la opción **-v** podrá refrescar éste periodo de tiempo sin necesidad de tener que ejecutar un mandato, en cuyo caso contrario expirará esta autenticación y será necesario volver a realizar ésta.

```
sudo -v
```

Si el usuario ejecuta **sudo** con la opción **-k** (minúscula), se forzará que expire el periodo de tiempo, obligando a ingresar nuevamente la contraseña la siguiente vez que se utilice el mandato **sudo**.

```
sudo -k
```

Lo anterior puede ir acompañado de un mandato, es decir permite ejecutar un mandato y expirar el periodo (estableciendo la fecha de último uso a la fecha y hora actual) de tiempo de manera simultánea. La ejecución de lo anterior, en si puede requerir ingresar la contraseña del usuario regular si el tiempo ya ha expirado. Por lo general se utiliza de este modo en operaciones que se quiere asegurar sean siempre realizadas por un ser humano y jamás por un programa. Ejemplo:

```
sudo -k service cups restart
```

Si el usuario ejecuta **sudo** con la opción **-K** (mayúscula), se forzará que expire el periodo de tiempo por completo (elimina toda referencia de tiempo), obligando a ingresar nuevamente la contraseña la siguiente vez que se utilice el mandato **sudo**. A diferencia de la opción **-k** (minúscula), ésta sólo permite ser utilizada sin mandatos.

```
sudo -K
```

15.7. Facilitando la vida con aliases.

BASH (**B**ourne-**A**gain **Sh**ell) permite utilizar variables de entorno y aliases al iniciar la sesión. Un administrador responsable por lo general preferirá evitar utilizar la cuenta de root y en su lugar hará uso de una cuenta de usuario regular para utilizar mandatos diversos a través del mandato **sudo**, los cuales se pueden simplificar a través de aliases. Por ejemplo, si se quiere definir que se utilice el mandato sudo cada vez que se invoque al mandato **chkconfig**, se puede un alias que anteceda el mandato **sudo** antes del mandato **/sbin/chkconfig**, como en el siguiente ejemplo:

```
alias chkconfig="sudo /sbin/chkconfig"
```

Lo anterior permitirá ejecutar el mandato **chkconfig** utilizando el mandato **sudo**, **sin necesidad de teclear el mandato sudo en el intérprete de mandatos**.

15.7.1. CentOS, Fedora y Red Hat Enterprise Linux.

Puede crear diversos aliases que pueden ser de utilidad en el archivo **~/.bashrc** del usuario regular utilizado, los cuales permitirán utilizar automáticamente mandatos diversos con sudo.

```
# .bashrc

# Source global definitions
if [ -f /etc/bashrc ]; then
        . /etc/bashrc
fi

# User specific aliases and functions

alias chgrp="sudo /bin/chgrp"
alias chkconfig="sudo /sbin/chkconfig"
alias chmod="sudo /bin/chmod"
alias chown="sudo /bin/chown"
alias depmod="sudo /sbin/depmod"
alias edquota="sudo /usr/sbin/edquota"
alias groupadd="sudo /usr/sbin/groupadd"
alias groupdel="sudo /usr/sbin/groupdel"
alias htpasswd="sudo /usr/bin/htpasswd"
alias ip="sudo /sbin/ip"
alias less="sudo /usr/bin/less"
alias openssl="sudo /usr/bin/openssl"
alias service="sudo /sbin/service"
alias system-config-firewall="sudo /usr/bin/system-config-firewall"
alias system-config-network-tui="sudo /usr/sbin/system-config-network-tui"
alias system-config-printer="sudo /usr/sbin/system-config-printer"
alias tail="sudo /usr/bin/tail"
alias useradd="sudo /usr/sbin/useradd"
alias userdel="sudo /usr/sbin/userdel"
alias vi="sudo /usr/bin/vim"
alias yum="sudo /usr/bin/yum"
```

Para que surtan efectos los cambios, hay que salir de la sesión y volver a ingresar con la misma cuenta de usuario en cuyo archivo **~/.bashrc** se añadieron estos aliases.

15.7.2. En openSUSE y SUSE Linux Enterprise.

Puede crear diversos aliases que pueden ser de utilidad en el archivo **~/.aliases** del usuario regular utilizado, los cuales permitirán utilizar automáticamente mandatos diversos con sudo.

```
alias chgrp="sudo /bin/chgrp"
alias chkconfig="sudo /sbin/chkconfig"
alias chmod="sudo /bin/chmod"
alias chown="sudo /bin/chown"
alias depmod="sudo /sbin/depmod"
alias edquota="sudo /usr/sbin/edquota"
alias groupadd="sudo /usr/sbin/groupadd"
alias groupdel="sudo /usr/sbin/groupdel"
alias htpasswd="sudo /usr/bin/htpasswd"
alias insserv="sudo /sbin/insserv"
alias ip="sudo /sbin/ip"
alias less="sudo /usr/bin/less"
alias openssl="sudo /usr/bin/openssl"
alias service="sudo /sbin/service"
alias tail="sudo /usr/bin/tail"
alias useradd="sudo /usr/sbin/useradd"
alias userdel="sudo /usr/sbin/userdel"
alias vi="sudo /usr/bin/vim"
alias yast="sudo /usr/sbin/yast2"
alias zypper="sudo /usr/bin/zypper"
```

Para que surtan efectos los cambios, hay que salir de la sesión y volver a ingresar con la misma cuenta de usuario en cuyo archivo **~/.aliases** se añadieron estos aliases.

16. Gestión de cuentas de usuario

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

16.1. Introducción.

Aún cuando se tenga un sistema con un único usuario, es importante recordar que es poco conveniente realizar el trabajo diario utilizando la cuenta del usuario **root**. Ésta sólo debe utilizarse para realizar las tareas de administración del sistema.

Una cuenta de **usuario regular** tiene las restricciones necesarias para impedir que se ejecuten mandatos que puedan dañar el sistema, se altere accidentalmente la configuración de éste, los servicios que trabajan en segundo plano o los permisos y ubicación de los archivos y directorios de sistema, etc. Sólo el usuario **root** tiene privilegios, sin restricciones, sobre el sistema.

16.2. Procedimientos.

La gestión de cuentas usuarios se puede realizar a través de los mandatos **useradd**, **passwd**, **usermod** y **groupmod**.

16.2.1. Gestión de cuentas de usuario.

16.2.1.1. Creación de cuentas de usuario.

Para crear una nueva cuenta de usuario, utilice el mandato **useradd** con la opción **-m** (crear automáticamente directorio de inicio) y el nombre del usuario como argumento. Ejemplo:

```
useradd -m pruebas
```

16.2.1.2. Asignación o cambio de contraseñas.

Establecer o cambiar una contraseña se ejecuta el mandato **passwd** con el nombre del usuario como argumento. Ejemplo:

```
passwd pruebas
```

El sistema solicitará ingrese la nueva contraseña para el usuario y que repita ésta para confirmar. Jamás se mostrarán los caracteres ingresados en pantalla. Si se sospecha se cometieron errores de tecleado, puede presionarse la tecla de retroceso las veces que sean necesarias y repetir todo lo que sea necesario antes de pulsar la tecla ENTER. El sistema siempre le informará si falla la confirmación de la contraseña devolviendo una salida **code 0** si el procedimiento fue exitoso o bien devolviendo una salida **code 1** si el procedimiento falló.

Sólo se permite al usuario root asignar contraseñas débiles mostrando siempre una advertencia cuando el caso lo amerite. En cambio, los usuarios regulares están obligados a asignar siempre una que sea segura y que excluya palabras incluidas en los diccionarios del sistema cuando realizan el procedimiento de cambio de contraseña.

16.2.1.3. Eliminación de cuentas de usuario.

Para eliminar una cuenta de usuario se ejecuta el mandato **userdel** con el nombre del usuario como argumento. Ejemplo:

```
userdel pruebas
```

Si se desea eliminar también el directorio de inicio del usuario, junto con su contenido, así como también el buzón de correo correspondiente, se debe ejecutar el mandato **userdel**, con la opción **-r** y el nombre del usuario como argumento. Ejemplo:

```
userdel -r pruebas
```

16.2.2. Gestión de Grupos.

16.2.2.1. Creación de grupos.

Se ejecuta el mandato **groupadd** con el nombre del grupo como argumento. Ejemplo:

```
groupadd grupo-que-sea
```

16.2.2.2. Creación de grupos de sistema.

Un grupo de sistema es aquel que tiene un número de identidad de grupo (GID) por debajo del 500 (CentOS y Red Hat™ Enterprise Linux) o bien 1000 (Fedora™, openSUSE™ y SUSE™ Linux Enterprise), dependiendo del sistema operativo utilizado. El número de identidad de grupo siempre se asigna automáticamente, utilizando el valor consecutivo más bajo que esté disponible en el sistema.

```
groupadd -r grupo-que-sea
```

16.2.2.3. Eliminación de grupos

Se ejecuta el mandato **groupdel** con el nombre del grupo como argumento. Ejemplo:

```
groupdel grupo-que-sea
```

16.2.2.4. Asignación de usuario existentes a grupos existentes.

Se ejecuta el mandato **gpasswd** con la opción **-a**, el nombre del usuario y el nombre del grupo como argumentos, en ese orden. Ejemplo:

```
gpasswd -a usuario-que-sea grupo-que-sea
```

16.2.3. Opciones avanzadas.

Pueden utilizarse las siguientes opciones del mandato **useradd**:

-c, --comment comentario

Establece una descripción de la cuenta de usuario. Actualmente se utiliza para definir el nombre completo del usuario.

-d, --home directorio de inicio

Establece el directorio de inicio del usuario.

-e, --expiredate fecha de expiración

Establece las fecha de expiración de una cuenta de usuario. Esta debe ingresarse en el siguiente formato: AAAA-MM-DD.

-f, --inactive días para desactivar

Establece el número de días para desactivar una cuenta de usuario tras la expiración de una contraseña.

-g, --gid grupo principal

Establece el grupo predeterminado al cual pertenecerá el usuario. Nota: el grupo definido debe de existir previamente.

-G, --groups grupos adicionales,[...]

Establece los grupos adicionales a los que pertenecerá el usuario. Estos deben separarse utilizando una coma y sin espacios. Esto es muy conveniente cuando se desea que el usuario tenga acceso a determinados recursos del sistema, como acceso a la unidad de disquetes, administración de cuentas PPP y POP. Nota: los grupos definidos deben de existir.

-m, --create-home

Establece el directorio de inicio del usuario debe ser creado si acaso este fuese inexistente y se copiaran dentro de este los archivos especificados en **/etc/skel**. Esta opción viene implícita en CentOS, Fedora™ y Red Hat™ Enterprise Linux, es decir es innecesaria, pues el archivo **/etc/login.defs** define la variable **CREATE_HOME** con el valor **yes**. Ejemplo:

```
useradd alguien.
```

En Debian, openSUSE™, SUSE™ Linux Enterprise y Ubuntu™, es necesario utilizarla de manera explícita, siendo que de lo contrario se omitiría la creación de los directorios de inicio de los usuarios, pues el archivo **/etc/login.defs** define la variable **CREATE_HOME** con el valor **no**. Ejemplo:

```
useradd -m alguien.
```

-M

Establece se omita crear el directorio de inicio del usuario, aún si el archivo **/etc/login.defs** define la variable **CREATE_HOME** con el valor **yes**. Es lo contrario de la opción **-m**.

-r, --system

Crea cuentas de sistema. Los usuarios de sistema serán creados sin caducidad en el archivo **/etc/shadow** y sus números de identidad serán asignados entre el rango de valores de la variable **SYS_UID_MIN** y la variable **SYS_UID_MAX** (100 a 499 en CentOS y Red Hat™ Enterprise Linux, 100 y 999 en Fedora™, openSUSE™ y SUSE™ Linux Enterprise) o bien como esté definido en el archivo **/etc/login.defs**.

-s, --shell intérprete de mandatos

Establece el intérprete de mandatos (*shell*) que podrá utilizar el usuario. CentOS, Red Hat™ Enterprise Linux, Fedora™, openSUSE™ y SUSE™ Linux Enterprise establecen **/bin/bash** como intérprete de mandatos predeterminado.

-u, --uid número de identidad de usuario

Establece el UID del usuario. Cuando se crea una cuenta de usuario por primera vez, como ocurre en CentOS y Red Hat™ Enterprise Linux, los UID se asignarán a partir del **500**. Los UID entre 0 y 99 están reservados para las cuentas y grupos de los servicios del sistema. En el caso de openSUSE™ y SUSE™ Linux Enterprise, éstos asignan los UID a partir del 1000. El rango de valores de SYS_UID_MIN-SYS_UID_MAX puede consultarse en el archivo **/etc/login.defs**.

Ejemplo:

```
useradd -c "Fulano de tal" \
    -u 1000 -m -d /home/pruebas \
    -G floppy,lp \
    pruebas
```

Lo anterior creará una cuenta de usuario llamada pruebas, que se encuentra incluido en los grupos **floppy** y **lp**, que tendrá un UID=1000, utilizará **/bin/bash** como intérprete de mandatos y utilizará /home/pruebas directorio de inicio.

La descripción completa de opciones para el mandato **useradd** puede consultarse en la página de manual correspondiente.

```
man 8 useradd
```

Para modificar una cuenta de usuario existente, se utiliza el mandato **usermod**, el cual tiene las siguientes opciones, que son similares a las del mandato **useradd**:

-c, --comment comentario

Cambia una descripción de la cuenta de usuario.

-d, --home directorio de inicio

Cambia el directorio de inicio del usuario.

-e, --expiredate fecha de expiración

Cambia las fecha de expiración de una cuenta de usuario. Esta debe ingresarse en el siguiente formato: AAAA-MM-DD.

-f, --inactive días para desactivar

Cambia el número de días para desactivar una cuenta de usuario tras la expiración de una contraseña.

-g, --gid grupo principal

Cambia el grupo predeterminado al cual pertenecerá el usuario. Nota: el grupo definido debe de existir previamente.

-G, --groups grupos adicionales,[...]

Cambia los grupos adicionales a los que pertenecerá el usuario. Estos deben separarse utilizando una coma y sin espacios. Nota: los grupos definidos deben de existir.

-l, --login nuevo nombre del usuario

Cambia el nombre del usuario.

-m, --move-home

Mueve el contenido del directorio de inicio del usuario cuando se ha establecido uno distinto con la opción -d.

-s, --shell intérprete de mandatos

Cambia el intérprete de mandatos (*shell*) que podrá utilizar el usuario.

-u, --uid número de identidad de usuario

Cambia el UID del usuario.

Ejemplo:

```
useramod -c "Alguien" \
    -s /bin/zsh \
    -u 1001 -m -d /home/alguien \
    -l alguien \
    pruebas
```

Lo anterior cambiará la cuenta del usuario llamada pruebas para que adelante tenga como descripción «Alguien», tenga el UID=1001, utilice /bin/zsh como intérprete de mandatos y cambie su directorio de inicio, moviendo todo su contenido, a /home/alguien.

La descripción completa de opciones para el mandato **usermod** puede consultarse en la página de manual correspondiente.

```
man 8 usermod
```

Pueden utilizarse las siguientes opciones del mandato **passwd**:

-k

Se utiliza para indicar que la actualización de una contraseña sólo se aplique para las sesiones expiradas, sin afectar a las sesiones activas del usuario modificado.

-l

Sólo puede ser utilizada por root. Se utiliza para bloquear cuentas de usuario. El bloqueo se realiza añadiendo el símbolo ! al inicio del criptograma de la contraseña en el archivo **/etc/shadow**.

--stdin

Establece que el mandato passwd deberá leer el valor de la contraseña desde la entrada estándar (STDIN).

-u

Sólo puede ser utilizada por root. Revierte lo que se haya hecho con la opción -l. Es decir, desbloquea cuentas de usuario. Es decir, elimina el símbolo ! al inicio del criptograma de la contraseña en el archivo **/etc/shadow**

-d

Sólo puede ser utilizada por root. Elimina la contraseña de un usuario en particular, permitiendo ingresar al sistema sin contraseña.

-e

Sólo puede ser utilizada por root. Expira la contraseña del usuario, obligando a éste a asignar una nueva durante el siguiente ingreso al sistema. Esta opción fue descartada en versiones recientes de passwd en favor del uso del mandato chage con la opción -d con el número cero como valor y el nombre del usuario como argumento. Ejemplo: `chage -d 0 zutano`.

-n tiempo mínimo de vida en días

Sólo puede ser utilizada por root. Establece el tiempo mínimo de vida, en días, de una contraseña.

-x tiempo máximo de vida en días

Sólo puede ser utilizada por root. Establece el tiempo máximo de vida, en días, de una contraseña.

-w número de días previos a expiración

Sólo puede ser utilizada por root. Establece el número de días, antes de que expire una contraseña, para que el usuario comience a recibir advertencias sobre la próxima expiración de su contraseña.

-i número de días tras la expiración de contraseña

Sólo puede ser utilizada por root. Establece el número de días para desactivar una cuenta de usuario tras la expiración de su contraseña.

-S

Sólo puede ser utilizada por root. Mostrará información breve acerca del estado de una contraseña para un usuario determinado.

Ejemplo:

```
passwd -n 60 -x 90 -w 10 -i 5 pruebas
```

Lo anterior establece que la contraseña del usuario pruebas tendrá un tiempo de vida mínimo de 60 días, un tiempo máximo de vida de 90 días, comenzará a recibir advertencias 10 días antes de que expire su contraseña y se desactivará la cuenta 5 días después de que caduque la contraseña en el caso de que el usuario hubiese omitido cambiarla.

La descripción completa de opciones para el mandato **passwd** puede consultarse en la página de manual correspondiente.

```
man 1 passwd
```

16.3. Comentarios finales acerca de la seguridad.

Cuando un intruso consigue infiltrarse en un sistema es generalmente es gracias a que se realizó una conexión a través de SSH o Telnet y se pudo "**adivinar**" alguna de las contraseñas de las cuentas de usuario existentes o bien la contraseña del administrador. Si se específico una **mala** contraseña de **root** durante el proceso de instalación del sistema operativo, algo muy común entre usuarios novicios, es muy probable que ésta sea vulnerada en pocas horas (e incluso minutos) después de conectarse a Internet.

- Evite especificar contraseñas fáciles de adivinar. Particularmente, evite utilizar contraseñas que utilicen palabras incluidas en cualquier diccionario de cualquier idioma, datos relacionados con el usuario o empresa, como son registro federal de contribuyentes (R.F.C.), fechas de nacimiento, números telefónicos, seguro social, números de cuentas de académicos o alumnos, nombres de mascotas, nombres de personajes de ciencia ficción, etc.

- Evite escribir las contraseñas sobre medios físicos, prefiera siempre limitarse a memorizar éstas.

- Si necesita almacenar contraseñas en un archivo, hágalo utilizando un buen cifrado.

- Si se le dificulta memorizar contraseñas complejas, utilice entonces contraseñas fáciles de recordar, pero **cámbielas periódicamente**.

- Jamás proporcione una contraseña a terceros. Evite proporcionarla en especial a personas que se identifiquen como miembros de algún servicio de soporte o ventas. Este último caso se menciona con énfasis en la página de manual del mandato **passwd**.

Se considera como una **buena** contraseña aquella se compone de una combinación de números y letras mayúsculas y minúsculas y que contiene como mínimo 8 caracteres, al menos tres caracteres en mayúscula, al menos tres números y al menos tres caracteres especiales. También es posible utilizar pares de palabras con puntuación insertada y frases o secuencias de palabras o bien acrónimos de estas.

Observar estas recomendaciones, principalmente en sistemas con acceso a redes locales y/o públicas, como Internet, hará que el sistema sea más seguro.

16.4. Configurando valores predeterminados para el alta de cuentas de usuario.

16.4.1. Archivo /etc/default/useradd.

Como *root* edite el archivo **/etc/default/useradd**:

```
vim /etc/default/useradd
```

Encontrará, invariablemente, el siguiente contenido:

```
# useradd defaults file
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
```

Puede cambiar lo valores que considere convenientes.

16.4.1.1. Variable HOME.

El directorio de inicio del usuario será creado dentro de /home, de acuerdo a como se estipula en **Estándar de Jerarquía de Sistema de Archivos** o **FHS** (**F**ilesystem **H**ierarchy **S**tandard). El valor de esta variable puede ser cambiado de acuerdo a las necesidades o preferencias del administrador.

Por ejemplo, en el caso de un sistema dedicado al servicio de hospedaje de anfitriones virtuales a través de un servidor HTTP, pudiera preferirse utilizar el directorio **/var/www** para este fin, con la finalidad de simplificar tareas para el administrador del sistema.

En otros casos, específicamente en servidores de correo, donde se quiere aplicar una sola **cuota de disco** general para buzón de correo y carpetas de correo en el directorio de inicio, pudiera crearse un directorio dentro del directorio **/var**, como por ejemplo el directorio **/var/home** o **/var/users**, de modo que al aplicar cuota de disco sobre la partición correspondiente al directorio **/var**, ésta involucraría tanto el buzón de entrada del usuario, correspondiente al archivo **/var/spool/mail/usuario**, así como también las carpetas de correo en el directorio de inicio del usuario, que teóricamente estarían localizadas dentro del directorio **/var/home/usuario/mail/**.

16.4.1.2. Variable SHELL.

El intérprete de mandatos a utilizar para las nuevas cuentas que sean creadas en adelante se define a través de la variable **SHELL**. De modo predeterminado el sistema asigna /bin/bash (BASH o **B**ourne **A**gain **Sh**ell) como intérprete de mandatos; si el sistema se utiliza como servidor, lo más conveniente es asignar otro valor predeterminado.

El valor más conveniente para la variable SHELL **/sbin/nologin**, el cual es un programa que de forma cortés rechaza el ingreso del usuario al sistema (login). Muestra brevemente un mensaje respecto a que la cuenta está desactivada (o bien cualquier mensaje que se se defina en el archivo **/etc/nologin.txt**) y obliga a una salida. Suele utilizarse como reemplazo de del intérprete de mandatos regular para cuentas de usuario que han sido desactivadas o bien que a las cuales se quiere impedir el acceso hacia un intérprete de mandatos. Este programa registra todo intento de acceso en la bitácora general del sistema, almacenada en el archivo /**var/log/messages**. Para utilizarlo como valor predeterminado para la variable **SHELL**, sólo hay que cambiar **SHELL=/bin/bash** por **SHELL=/sbin/nologin**.

```
# useradd defaults file
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/sbin/nologin
SKEL=/etc/skel
```

Una vez terminada la edición, en adelante todo nuevo usuario que sea dado de alta en el sistema con el mandato *useradd,* sin definir parámetro alguno, de modo predeterminado se le impedirá el acceso al sistema a través de una consola o terminal. Los usuarios con estas características podrán, sin embargo, utilizar cualquier otro servicios como FTP, correo o Samba sin problema alguno.

Los posibles valores para la variable SHELL pueden ser:

- **/sbin/nologin**, programa que de forma cortés rechaza el ingreso en el sistema (login).
- **/bin/false**, programa que realiza salida inmediata indicando falla. Es decir, que impide el acceso al sistema y además con devuelve falla. Es ideal si se quiere tener cuentas de usuario sólo con acceso hacia FTP, correo, Samba, etc., sin acceso hacia el intérprete de mandatos.
- **/dev/null**, el dispositivo nulo descarta todos los datos escritos sobre éste y para cualquier proceso que lo utilice. Es ideal para cuentas de usuario para las cuales sólo se quiere acceso a correo electrónico (SMTP, POP3, IMAP y/o cliente de correo con interfaz HTTP).
- **/bin/bash**, intérprete de mandatos desarrollado por el proyecto GNU. Es el intérprete de mandatos predeterminado en GNU/Linux.
- **/bin/sh**, un enlace simbólico que apunta hacia **/bin/bash** y ofrece una versión simplificada de Bash muy similar a Bourne Shell (sh).
- **/bin/tcsh**, una versión mejorada del intérprete de mandatos de C (csh).
- **/bin/ash**, un clon de Bourne shell (sh) que utiliza menos memoria.
- **/bin/zsh**, una versión mejorada de sh con funciones útiles encontradas en Bash y tcsh.

16.4.2. Directorio /etc/skel.

De modo predeterminado las cuentas de usuario del sistema utilizarán como plantilla al directorio **/etc/skel** para crear el directorio de inicio de todos los usuarios del sistema. En sistemas basados sobre CentOS, Fedora™, Red Hat™ Enterprise Linux, regularmente y como mínimo, el directorio **/etc/skel** incluye los siguientes archivos:

```
.bash_logout  .bash_profile  .bashrc  .gtkrc
```

Si, por ejemplo, se desea que cada nueva cuenta de usuario incluya un directorio subordinado para carpetas de correo electrónico y además el archivo para la suscripción de éstas a través del servicio de IMAP, se debe realizar el siguiente procedimiento:

```
mkdir -m 0700 /etc/skel/mail/
```

```
touch /etc/skel/mail/Drafts
touch /etc/skel/mail/Junk
touch /etc/skel/mail/Sent
touch /etc/skel/mail/Trash
chmod 600 /etc/skel/mail/*
```

Utilice cualquier editor de texto para crear el archivo **/etc/skel/mail/.subscriptions**:

```
vim /etc/skel/mail/.subscriptions
```

Este archivo sirve para registrar las suscripciones hacia carpetas de correo electrónico que serán utilizadas por el servicio IMAP. Añada el siguiente contenido:

```
INBOX
Drafts
Junk
Sent
Trash
```

A fin de que éste archivo tenga la seguridad necesaria, asigne a éste un permiso 600 (rw-------):

```
chmod 600 /etc/skel/mail/.subscriptions
```

16.5. Ejercicio: Creando cuentas de usuario.

16.5.1. Introducción

A fin de poder trabajar con comodidad, se crearán algunos grupos y cuentas de usuario con diversas características.

16.5.2. Procedimientos

1. Genere, al usuario denominado «fulano» con /bin/bash como intérprete de mandatos, directorio de inicio **/home/fulano** y grupo principal fulano (valores por defecto):

```
useradd -m -s /bin/bash -c "Fulano de Tal" fulano


passwd fulano
```

2. Genere al usuario denominado «mengano» definiendo /dev/null como intérprete de mandatos, asignando el directorio de inicio **/home/mengano** y grupo principal «mengano» (valores por defecto):

```
useradd -m -s /dev/null -c "Mengano de Tal" mengano


passwd mengano
```

3. Genere el grupo denominado «desarrollo»:

```
groupadd desarrollo
```

4. Genere el grupo denominado «sistemas» como grupo de sistema:

```
groupadd -r sistemas
```

5. Genere al usuario denominado «perengano» definiendo /sbin/nologin como intérprete de mandatos, asignando el directorio de inicio /home/perengano, grupo principal de desarrollo y grupo adicional sistemas:

```
useradd -m -s /sbin/nologin \
     -d /home/perengano -g desarrollo \
     -G sistemas \
     -c "Perengano de Tal" perengano


passwd perengano
```

6. Genere al usuario denominado «zutano» con /bin/bash como intérprete de mandatos, asignando el directorio de inicio /home/zutano, grupo principal sistemas, grupo adicional de desarrollo y defina que su contraseña expira de inmediato para que se force al usuario zutano a establecer una nueva contraseña con su siguiente ingreso al sistema:

```
useradd -m -s /bin/bash \
     -d /home/zutano -g sistemas \
     -G desarrollo \
     -c "Zutano de Tal" zutano


passwd zutano


passwd -e zutano || chage -d 0 zutano
```

7. Visualice el contenido de los archivos **/etc/group, /etc/passwd** y **/etc/shadow** y compare y determine las diferencias entre los grupos «desarrollo» y «sistemas» y los usuarios «fulano», «mengano», «perengano» y «zutano».

```
tail -2 /etc/group
tail -4 /etc/passwd
tail -4 /etc/shadow
```

17. Breve lección de mandatos básicos.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales (incluyendo su publicación, a través de cualquier medio, por entidades con fines de lucro). c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en castellano. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

17.1. Introducción.

Por favor, **siga los procedimientos al pie de la letra**. En varios ejemplos utilizará el carácter ~ (tilde), que es una forma de abreviar el directorio de inicio del usuario utilizado.

Ingrese como **root** y verifique que estén instalados los paquetes man, perl, less, file y man-pages-es

Si utiliza **CentOS**, **Fedora™** o **Red Hat™ Enterprise Linux**, ejecute lo siguiente:

```
yum -y install man perl less file man-pages-es finger
```

Si utiliza **openSUSE™** o **SUSE™ Linux Enterprise**, ejecute lo siguiente:

```
yast -i man perl less file man-pages finger
```

Si utiliza **CentOS** o **Red Hat™ Enterprise Linux** ejecute el mandato **makewhatis** para generar un índice de las páginas de manual presentes en el sistema.

```
makewhatis
```

Si utiliza **Fedora™**, **openSUSE™** o **SUSE™ Linux Enterprise** ejecute el mandato **mandb** para generar un índice de las páginas de manual presentes en el sistema.

```
mandb
```

Espere unos minutos a que termine de generarse el índice de manuales.

Cierre la sesión de root ejecutando el mandato exit:

```
exit
```

17.2. Procedimientos.

Ingrese al sistema como usuario regular (fulano).

17.2.1. Cambiar de usuario a super-usuario.

Ejecute el mandato **su** sin argumentos e ingrese la clave de acceso de **root** cuando se le solicite:

```
su
```

Ejecute lo siguiente para ver las variables de entorno:

```
echo $USER; echo $LOGNAME; echo $SHELL; echo $PATH; echo $HOME
```

Lo anterior debe devolver la siguiente salida:

```
fulano
fulano
/bin/bash
/usr/local/bin:/usr/bin:/bin:/usr/local/sbin:/usr/sbin:/sbin:/home/fulano/bin
/root
```

Observe que aunque se tienen privilegios de **root**, se carece de las variables de entorno de éste, por lo cual algunos mandatos sólo se podrán ejecutar si se específica la rutas exacta de éstos (ejemplos: /sbin/service, /sbin/chkconfig, /sbin/fsck y /sbin/fdisk).

Ejecute el mandato exit.

```
exit
```

Ejecute el mandato **su**, esta vez con la opción **-l** (que es lo mismo que «**su -**» o bien «**su --login**») e ingrese la clave de acceso de **root** cuando se le solicite:

```
su -l
```

Ejecute lo siguiente para ver las variables de entorno:

```
echo $USER; echo $LOGNAME; echo $SHELL; echo $PATH; echo $HOME
```

Lo anterior debe devolver la siguiente salida:

```
root
root
/bin/bash
/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin
/root
```

Observe que además de los privilegios de **root**, se tienen también de las variables de entorno de éste, pues en realidad se ha realizado un ingreso (login) como **root**.

Ejecute el mandato **exit** para regresar como usuario regular (fulano).

```
exit
```

17.2.2. Ver información del sistema y usuarios.

Ejecute:

```
uname -a
```

Lo anterior devolverá una salida similar a la siguiente, en la cual se mostrará el nombre del núcleo, nombre de anfitrión, número de lanzamiento del núcleo, versión del núcleo de Linux, tipo de microprocesador, plataforma del sistema y nombre del sistema operativo.

```
Linux localhost.localdomain 2.6.32-71.29.1.el6.i686 #1 SMP Mon Jun 27 18:07:00 BST 2011
i686 i686 i386 GNU/Linux
```

Ejecute lo siguiente para identificar cuál es el nombre de usuario que está usted está utilizando en el sistema:

```
whoami
```

Ejecute lo siguiente para visualizar cuáles usuarios están conectados en el sistema y dónde lo están haciendo:

```
who
```

Ejecute lo siguiente para visualizar cuáles usuarios están conectados en el sistema, en qué tipo de terminal lo están haciendo y qué es lo que están haciendo:

```
w
```

Ejecute lo siguiente para visualizar cuáles usuarios están conectados en el sistema, en qué tipo de terminal lo están haciendo y mostrar la información de usuario definida en el archivo **/etc/passwd**:

```
finger
```

Ejecute lo siguiente para ver la bitácora de acceso de los más recientes ingresos a sistema de todos los usuarios existentes en el sistema, es decir un resumen del contenido del archivo **/var/log/lastlog**:

```
lastlog
```

Ejecute lo siguiente para visualizar la bitácora de accesos hacia el sistema, es decir un extracto del contenido del archivo **/var/log/wtmp**:

```
last
```

Ejecute lo siguiente para ver con privilegios de root el resumen de la bitácora de intentos fallidos de acceso al sistema, es decir un resumen del contenido del archivo **/var/log/btmp**:

```
su -l root -c "lastb"
```

17.2.3. Operaciones con archivos y directorios.

Ejecute:

```
file /etc/hosts
```

Lo anterior devolverá que /etc/hosts es un archivo de texto.

```
/etc/hosts: ASCII text
```

Ejecute:

```
file /boot/grub/e2fs_stage1_5
```

Lo anterior devolverá que /boot/grub/e2fs_stage1_5 es un archivo de GRand Unified Bootloader y otras propiedades.

```
/boot/grub/e2fs_stage1_5: GRand Unified Bootloader stage1_5 version 3.2, identifier
0x2, GRUB version 0.97, configuration file /boot/grub/stage2
```

Ejecute:

```
pwd
```

Lo anterior devolverá el directorio de trabajo actual, en este caso el directorio de inicio del usuario. El mandato **pwd** sirve para mostrar la ruta del directorio de trabajo actual (***p**ath of **w**orking **d**irectory*).

Cambie al directorio **/usr/local**/usr/local utilizando el mandato **cd**, el cual sirve para cambiar de directorio (***c**hange **d**irectory*):

```
cd /usr/local
```

Ejecute el mandato **pwd**:

```
pwd
```

Lo anterior mostrará el directorio de trabajo actual.

Para regresar a su directorio de inicio (~), ejecute el mandato cd sin argumentos:

```
cd
```

Ejecute nuevamente el mandato **pwd** para verificar que se encuentra en su directorio de inicio:

```
pwd
```

Lo anterior deberá mostrar que ahora se encuentra dentro de su directorio de inicio (~).

Ejecute:

```
ls /usr/local
```

Lo anterior mostrará el contenido del directorio **/usr/local** y demostrará que es innecesario cambiarse a un directorio en particular, sólo para ver su contenido. El mandato **ls** sirve para listar el contenido del sistema de archivos (***l**i**s**t*)

Ejecute:

```
ls
ls -a
```

Primero se mostrará que el directorio de inicio (~) está vacío; después se mostrará que en realidad si hay contenido; los archivos y directorios de convierten a ocultos al re-nombrar éstos, poniendo un punto al inicio de su nombre.

```
.   .bash_history  .bash_profile  .gnome2   .Xauthority
..  .bash_logout   .bashrc        .mozilla
```

Ejecute:

```
ls -la
```

Lo anterior mostrará todo el contenido de su directorio de inicio (~), en una lista ordenada por nombre, la cual mostrará además tamaños en bytes, atributos y permisos:

```
total 24
drwx------. 4 fulano fulano 4096 sep 23 21:22 .
drwxr-xr-x. 5 root   root   4096 sep 23 20:51 ..
-rw-------. 1 fulano fulano  143 sep 23 20:59 .bash_history
-rw-r--r--. 1 fulano fulano   18 may 30 11:58 .bash_logout
-rw-r--r--. 1 fulano fulano  176 may 30 11:58 .bash_profile
-rw-r--r--. 1 fulano fulano  124 may 30 11:58 .bashrc
```

Ejecute:

```
ls -lar
```

La salida será similar a la del mandato anterior, ordenando por nombre los archivos, pero en orden inverso:

```
total 24
-rw-r--r--. 1 fulano fulano  124 may 30 11:58 .bashrc
-rw-r--r--. 1 fulano fulano  176 may 30 11:58 .bash_profile
-rw-r--r--. 1 fulano fulano   18 may 30 11:58 .bash_logout
-rw-------. 1 fulano fulano  143 sep 23 20:59 .bash_history
drwxr-xr-x. 5 root   root   4096 sep 23 20:51 ..
drwx------. 4 fulano fulano 4096 sep 23 21:35 .
```

Ejecute:

```
ls -hlar
```

La salida será similar a la del mandato anterior, ordenando los archivos por nombre, en orden inverso, pero mostrando los tamaños de archivos en unidades más fáciles de entender:

```
total 24K
-rw-r--r--. 1 fulano fulano  124 may 30 11:58 .bashrc
-rw-r--r--. 1 fulano fulano  176 may 30 11:58 .bash_profile
-rw-r--r--. 1 fulano fulano   18 may 30 11:58 .bash_logout
-rw-------. 1 fulano fulano  143 sep 23 20:59 .bash_history
drwxr-xr-x. 5 root   root   4.0K sep 23 20:51 ..
drwx------. 4 fulano fulano 4.0K sep 23 21:35 .
```

Ejecute:

```
ls -Sla
```

Lo anterior deberá de mostrar todo el contenido del directorio de inicio (~), mostrará los atributos y permisos y ordenará los elementos por tamaño:

```
total 24
drwx------. 4 fulano fulano 4096 sep 23 21:35 .
drwxr-xr-x. 5 root   root   4096 sep 23 20:51 ..
-rw-r--r--. 1 fulano fulano  176 may 30 11:58 .bash_profile
-rw-------. 1 fulano fulano  143 sep 23 20:59 .bash_history
-rw-r--r--. 1 fulano fulano  124 may 30 11:58 .bashrc
-rw-r--r--. 1 fulano fulano   18 may 30 11:58 .bash_logout
```

Ejecute:

```
ls -Slar
```

La salida será similar a la del mandato anterior, ordenando los archivos por tamaño, pero en orden inverso:

```
total 24
-rw-r--r--. 1 fulano fulano   18 may 30 11:58 .bash_logout
-rw-r--r--. 1 fulano fulano  124 may 30 11:58 .bashrc
-rw-------. 1 fulano fulano  143 sep 23 20:59 .bash_history
-rw-r--r--. 1 fulano fulano  176 may 30 11:58 .bash_profile
drwxr-xr-x. 5 root   root   4096 sep 23 20:51 ..
drwx------. 4 fulano fulano 4096 sep 23 21:35 .
```

Ejecute:

```
ls -tla
```

Lo anterior deberá de mostrar todo el contenido del directorio de inicio (~), mostrará los atributos y permisos y ordenará los elementos por fecha de modificación:

```
total 24
drwx------. 4 fulano fulano 4096 sep 23 21:35 .
-rw-------. 1 fulano fulano  143 sep 23 20:59 .bash_history
drwxr-xr-x. 5 root   root   4096 sep 23 20:51 ..
-rw-r--r--. 1 fulano fulano   18 may 30 11:58 .bash_logout
-rw-r--r--. 1 fulano fulano  176 may 30 11:58 .bash_profile
-rw-r--r--. 1 fulano fulano  124 may 30 11:58 .bashrc
```

Ejecute:

```
ls -tlar
```

La salida será similar a la del mandato anterior, ordenando los archivos por fecha de modificación, pero en orden inverso:

```
total 24
-rw-r--r--. 1 fulano fulano  124 may 30 11:58 .bashrc
-rw-r--r--. 1 fulano fulano  176 may 30 11:58 .bash_profile
-rw-r--r--. 1 fulano fulano   18 may 30 11:58 .bash_logout
drwxr-xr-x. 5 root   root   4096 sep 23 20:51 ..
-rw-------. 1 fulano fulano  143 sep 23 20:59 .bash_history
drwx------. 4 fulano fulano 4096 sep 23 21:35 .
```

Ejecute:

```
ls -htlar
```

La salida será similar a la del mandato anterior, pero mostrando los tamaños de los archivos en unidades más fáciles de entender:

```
total 24K
-rw-r--r--. 1 fulano fulano  124 may 30 11:58 .bashrc
-rw-r--r--. 1 fulano fulano  176 may 30 11:58 .bash_profile
-rw-r--r--. 1 fulano fulano   18 may 30 11:58 .bash_logout
drwxr-xr-x. 5 root   root   4.0K sep 23 20:51 ..
-rw-------. 1 fulano fulano  143 sep 23 20:59 .bash_history
drwx------. 4 fulano fulano 4.0K sep 23 21:35 .
```

Ejecute:

```
ls -ia
```

La salida será similar a la del mandato anterior, pero mostrando la información del número de inodo que corresponden a cada uno de los archivos del directorio de trabajo actual:

```
4194305 .   4194307 .bash_history  4194306 .bash_profile
      2 ..  4194315 .bash_logout   4194310 .bashrc
```

Ejecute:

```
ls -lia
```

La salida será similar a la del mandato anterior, mostrando la información del número de inodo que corresponden a cada uno de los archivos del directorio de trabajo actual, con detalles:

```
total 24
4194305 drwx------ 2 fulano fulano 4096 jun 21 16:47 .
      2 drwxr-xr-x 9 root   root   4096 jun 21 16:42 ..
4194307 -rw------- 1 fulano fulano   63 jun 21 16:47 .bash_history
4194315 -rw------- 1 fulano fulano   18 mar 26 19:22 .bash_logout
4194306 -rw------- 1 fulano fulano  193 mar 26 19:22 .bash_profile
4194310 -rw------- 1 fulano fulano  124 mar 26 19:22 .bashrc
```

Ejecute lo siguiente para crear varios archivos vacíos:

```
touch archivo1 archivo2 archivo11 archivo12 archivo135 archivo246
touch archivoA archivoB archivoaa archivoAB archivoabc archivoABC
```

Ejecute:

```
ls archivo*1*
```

La salida de lo anterior deberá mostrar todos los archivos cuyo nombre inicia con la cadena **archivo** pero sólo aquellos que incluyen el número **1** después de la cadena archivo:

```
archivo1  archivo11  archivo12  archivo135
```

Ejecute:

```
ls archivo[!*1]*
```

La salida de lo anterior deberá mostrar todos los archivos cuyo nombre inicia con la cadena **archivo1** pero sólo aquellos que carecen del número **1** en cualquier parte después de la cadena archivo:

```
archivo2    archivoA   archivoAB   archivoB
archivo246  archivoaa  archivoabc  archivoABC
```

Ejecute:

```
ls archivo???
```

La salida de lo anterior deberá mostrar todos los archivos cuyo nombre inicia con la cadena **archivo** pero sólo aquellos que incluyen sólo tres caracteres adicionales después de la cadena archivo:

```
archivo135  archivo246  archivoABC  archivoABC
```

Ejecute:

```
ls archivo??
```

La salida de lo anterior deberá mostrar sólo los archivos cuyo nombre inicia con la cadena **archivo** pero sólo aquellos que incluyen sólo dos caracteres adicionales después de la cadena archivo:

```
archivo11  archivo12  archivoaa  archivoAB
```

Ejecute:

```
ls archivo[[:digit:]]*
```

La salida de lo anterior deberá mostrar sólo los archivos cuyo nombre inicia con la cadena **archivo** pero sólo aquellos que incluyen números después de la cadena archivo:

```
archivo1  archivo11  archivo12  archivo135  archivo2  archivo246
```

Ejecute:

```
ls archivo[[:lower:]]*
```

La salida de lo anterior deberá mostrar sólo los archivos cuyo nombre inicia con la cadena **archivo** pero sólo aquellos que terminan en letras minúsculas:

```
archivoaa  archivoabc
```

Ejecute:

```
ls archivo[[:upper:]]*
```

La salida de lo anterior deberá mostrar sólo los archivos cuyo nombre inicia con la cadena **archivo** pero sólo aquellos que terminan en letras mayúsculas:

```
archivoA  archivoAB  archivoB  archivoABC
```

Ejecute:

```
ls archivo*[![:digit:]]
```

La salida de lo anterior deberá mostrar sólo los archivos cuyo nombre inicia con la cadena **archivo** pero sólo aquellos que terminan en caracteres distintos a los números:

```
archivoA  archivoaa  archivoAB  archivoabc  archivoABC  archivoB
```

Ejecute:

```
ls archivo*[cC]
```

La salida de lo anterior deberá mostrar sólo los archivos cuyo nombre inicia con la cadena **archivo** pero sólo aquellos que terminan en c o C:

```
archivoabc  archivoABC
```

Ejecute:

```
ls archivo*[!cC]
```

La salida de lo anterior deberá mostrar sólo los archivos cuyo nombre inicia con la cadena **archivo** pero sólo aquellos que terminan con cualquier carácter excepto c o C:

```
archivo1   archivo12   archivo2    archivoA   archivoAB
archivo11  archivo135  archivo246  archivoaa  archivoB
```

Ejecute:

```
ls archivo[!aA1]*
```

La salida de lo anterior deberá mostrar sólo los archivos cuyo nombre inicia con la cadena **archivo** pero sólo aquellos que excluyen a, A o el número 1 después de la cadena archivo:

```
archivo2  archivo246  archivoB
```

Ejecute lo siguiente para crear un nuevo directorio:

```
mkdir ejemplos1
```

Ejecute lo siguiente para intentar generar otro directorio denominado «uno», pero dentro del directorio «ejemplos2» (el cual es inexistente).

```
mkdir ejemplos2/uno/
```

Lo anterior devolverá un mensaje de error como el siguiente:

```
mkdir: no se puede crear el directorio «ejemplos2/uno»: No existe el archivo o el
directorio
```

A fin de poder crear el directorio «uno», dentro del directorio «ejemplos2», es necesario crear primero «ejemplos2». Sin embargo puede indicarle a mkdir que genere toda la ruta añadiendo la opción -p (path):

```
mkdir -p ejemplos2/uno
ls
ls ejemplos2
```

Lo anterior creo el directorio «ejemplos2» y dentro de éste al directorio «uno» y mostró al directorio «ejemplos2» y mostró dentro de éste al directorio «uno».

Copie algunos archivos para experimentar con este directorio, utilizando el mandato *cp*:

```
cp /etc/fstab ~/ejemplos1/
```

Vuelva a utilizar el mandato **cp** de este modo:

```
cp /etc/passwd ~/ejemplos1/
```

Con estos dos procedimientos, se habrán copiado dos distintos archivos (**/etc/fstab** y **/etc/passwd**) dentro del directorio *ejemplos1*.

Intente copiar el directorio **~/ejemplos1/** como el nuevo directorio **~/copia1**, ejecutando lo siguiente:

```
cp ~/ejemplos1/ ~/copia1
```

Lo anterior devolverá un error porque ~/ejemplos1 es un directorio:

```
cp: se omite el directorio «ejemplos1/»
```

Para realizar la copia de un directorio, junto con todo su contenido, debe usar el mandato **cp** con la opción **-r**, lo cual realizará una copia recursiva del directorio de origen como el directorio de destino indicado. Ejecute lo siguiente:

```
cp -r ~/ejemplos1/ ~/copia1/
```

Visualice el contenido de ambos directorios utilizando el mandato **ls** con la opción **-l**:

```
ls -l ejemplos1/ copia1/
```

La salida le mostrará lo siguiente:

```
copia1/:
total 8
-rw-r--r-- 1 fulano fulano 1052 abr 27 10:58 fstab
-rw-r--r-- 1 fulano fulano 1957 abr 27 10:58 passwd

ejemplos1/:
total 8
-rw-r--r-- 1 fulano fulano 1052 abr 27 10:54 fstab
-rw-r--r-- 1 fulano fulano 1957 abr 27 10:54 passwd
```

Notará que las fechas de modificación de los archivos contenidos en ambos directorios son diferentes.

Elimine el directorio copia1, ejecutando lo siguiente:

```
rm -fr ~/copia1/
```

Para realizar una copia de un directorio, preservando todos los atributos y permisos del contenido del directorio original, utilice el mandato **cp** con la opción **-a**:

```
cp -a ~/ejemplos1/ ~/copia1/
```

Para realizar una copia de un directorio, preservando todos los atributos y permisos del contenido del directorio original, pero sólo copiando los archivos que cambiaron respecto de el directorio de origen y viendo una salida descriptiva, utilice el mandato **cp** con las opciones **-auv**:

```
cp -auv ~/ejemplos1/ ~/copia1/
```

Visualice de nuevo el contenido de ambos directorios utilizando el mandato **ls** con la opción **-l**:

```
ls -l ~/ejemplos1/ ~/copia1/
```

La salida le mostrará algo similar a lo siguiente:

```
copia1/:
total 8
-rw-r--r-- 1 fulano fulano 1052 abr 27 10:54 fstab
-rw-r--r-- 1 fulano fulano 1957 abr 27 10:54 passwd

ejemplos1/:
total 8
-rw-r--r-- 1 fulano fulano 1052 abr 27 10:54 fstab
-rw-r--r-- 1 fulano fulano 1957 abr 27 10:54 passwd
```

Notará que las fechas de modificación de los archivos contenidos en ambos directorios son idénticas.

Utilice el mandato **touch** para cambiar la fecha de modificación del archivo **~/ejemplos1/fstab**:

```
touch ~/ejemplos1/fstab
```

Utilice el mandato **cp** con las opciones **-a** para realizar una copia exacta del directorio de origen y sus contenidos, **-u** para realizar sólo la copia de los contenido nuevos y utilizando la opción **-v** para ver una salida detallada:

```
cp -auv ~/ejemplos1/* ~/copia1/
```

Lo anterior debe devolver una salida similar a la siguiente.

```
«ejemplos1/fstab» -> «copia1/fstab»
```

Utilice de nuevo el mandato **mkdir** y genere un directorio denominado **adicional** dentro del directorio de **ejemplos1**.

```
mkdir ~/ejemplos1/adicional
```

Acceda al directorio de *ejemplos1* para continuar. Ejecute lo siguiente:

```
cd ~/ejemplos1/
```

Liste el contenido de este directorio, ejecutando lo siguiente:

```
ls
```

Se mostrarán los archivos **fstab** y **passwd** y el directorio **adicional**.:

```
[fulano@localhost ejemplos1]$
adicional fstab  passwd
[fulano@localhost ejemplos1]$
```

Mueva el archivo fstab dentro del directorio **adicional** utilizando el mandato **mv**:

```
mv fstab adicional/
```

Examine el contenido del directorio **ejemplos1** utilizando de nuevo el mandato **ls**:

```
ls
```

Obtendrá una salida similar a la siguiente:

```
[fulano@localhost ejemplos1]$
adicional  passwd
[fulano@localhost ejemplos1]$
```

Acceda al directorio **adicional** con el mandato **cd**

```
cd adicional
```

Visualice el contenido del directorio de trabajo actual ejecutando el mandato **ls**.

```
ls
```

Se mostrará una salida similar a la siguiente:

```
[fulano@localhost adicional]$
fstab
[fulano@localhost adicional]$
```

Regrese al directorio **ejemplos1** que se encuentra en el nivel superior utilizando el mandato **cd**:

```
cd ../
```

Proceda a eliminar el archivo **passwd** que se encuentra en el directorio **ejemplos1**

```
rm passwd
```

Haga lo mismo con **fstab**, el cual se localiza dentro del directorio **adicional**:

```
rm adicional/fstab
```

Elimine el directorio **adicional**:

```
rmdir adicional
```

Genere un nuevo sub-directorio denominado **directorios1**:

```
mkdir directorios1
```

Cambie a este nuevo directorio:

```
cd directorios1
```

Ejecuta lo siguiente:

```
mkdir Nuevo Directorio
```

Liste el contenido del directorio de trabajo actual mostrando una sola columna:

```
ls -1
```

Lo anterior creó dos nuevos directorios, uno denominado **«Nuevo»** y otro denominado **«Directorio»**, por lo que verá una salida como la siguiente:

```
Directorio
Nuevo
```

Ejecuta lo siguiente, que será similar al último mkdir, pero que en esta ocasión utilizará una diagonal inversa antes del espacio:

```
mkdir Nuevo\ Directorio
```

Liste el contenido del directorio de trabajo actual mostrando una sola columna:

```
ls -1
```

Lo anterior creó un nuevo directorio denominado **«Nuevo Directorio»**, por lo que verá una salida como la siguiente:

```
Directorio
Nuevo
Nuevo Directorio
```

La diagonal inversa se utilizó como carácter de escape para indicar que espacio entre **«Nuevo»** y **«Directorio»** es parte del nombre el directorio que se quiere crear.

Puede lograrse el mismo efecto escribiendo el nombre del directorio a crear entre comillas. Ejecute lo siguiente:

```
mkdir "Otro Directorio"
```

Liste el contenido del directorio de trabajo actual mostrando una sola columna:

```
ls -1
```

Lo anterior creó un nuevo directorio denominado **«Otro Directorio»**, por lo que verá una salida como la siguiente:

```
Directorio
Nuevo
Nuevo Directorio
Otro Directorio
```

Regrese a su directorio de inicio.

```
cd
```

17.2.4. Consultar ayuda, páginas de manual e información.

Ejecute:

```
ls --help
```

Lo anterior mostrará la ayuda del mandato **ls**. Pulse simultáneamente las teclas «SHIFT» y «Re Pág» y luego las teclas «SHIFT» y «Av Pág»; ésto permitirá avanzar o retroceder en el documento.

Pulse la tecla «ENTER» y ejecute lo siguiente:

```
man ls
```

Lo anterior mostrará el manual en español. Pulse las teclas «Av Pág» y «Re Pág» para avanzar o retroceder. Pulse la tecla **/**, ingrese la cadena de texto «director» y pulse la tecla «ENTER»:

```
:/director
```

Lo anterior habrá realizado una búsqueda en el manual del mandato **ls** y resaltado las incidencias de la cadena de texto «director». Pulse la tecla **q** para salir.

Si necesita consultar otros manuales relacionados con el mandato **ls**, ejecute el mandato man con la opción -k y el nombre del mandato a consultar, del siguiente modo

```
man -k ls
```

Lo anterior devolverá una extensa salida que consistirá en la lista de todas las páginas de manual que incluyen información relacionada con el mandato **ls**.

Para obtener una lista más específica, ejecute lo siguiente:

```
whatis ls
```

Ejecute lo siguiente:

```
man -k crontab
```

Lo anterior devolverá una salida similar a la siguiente, la cual indica que hay dos distintos manuales para **crontab** (1 y 5).

```
crontab (1)          - maintains crontab files for individual users
crontab (5)          - files used to schedule the execution of programs
```

Las páginas de manual se organizan en las siguientes categorías:

- 1 corresponde a manuales para programas ejecutables y guiones del intérprete de mandatos.
- 2 corresponde a manuales para llamadas del sistema (funciones servidas por el núcleo).
- 3 corresponde a manuales para llamadas de la biblioteca (funciones contenidas en las bibliotecas del sistema).
- 4 corresponde a manuales para archivos especiales (se encuentran generalmente en /dev).
- 5 corresponde a manuales para formato de archivos y convenios.

- 6 corresponde a manuales para juegos
- 7 corresponde a manuales para paquetes de macros y convenios.
- 8 corresponde a manuales para mandatos de administración del sistema (generalmente sólo son para root)
- 9 corresponde a manuales para rutinas del núcleo [No es estándar]
- n se utilizaba en el pasado para clasificar las páginas de manual nuevas. Hoy en día es obsoleto.
- l se utilizaba en el pasado para clasificar las páginas de manual para uso local. Hoy en día es obsoleto.
- p se utilizaba en el pasado para clasificar las páginas de manual públicas. Hoy en día es obsoleto.
- o se utilizaba en el pasado para clasificar las páginas de manual antiguas. Hoy en día es obsoleto.

Lo que significa que **crontab(1)** corresponde al manual del programa **crontab** y **crontab(5)** corresponde al manual del formato del archivo **/etc/crontab**. Para consultar éste último ejecute lo siguiente:

```
man 5 crontab
```

Para salir, pulse la tecla **q**.

Ejecute lo siguiente:

```
info ls
```

Lo anterior mostrará la página de información del mandato **ls**. El mandato info se se puede utilizar cuando se carece de páginas de manual. Para salir, pulse la tecla **q**.

17.2.5. Visualizando contenido de archivos.

Regrese a su directorio de inicio.

```
cd
```

Ejecute:

```
wc -m /etc/crontab
```

Lo anterior devolverá que el archivo /etc/crontab contiene cierto número de carácteres.

Ejecute:

```
wc -w /etc/crontab
```

Lo anterior devolverá que el archivo /etc/crontab contiene cierto número de palabras.

Ejecute:

```
wc -l /etc/crontab
```

Lo anterior devolverá que el archivo /etc/crontab contiene cierto número de líneas.

Ejecute:

```
wc -L /etc/crontab
```

Lo anterior devolverá que la línea más larga del archivo /etc/crontab tiene cierto número de carácteres.

Ejecute:

```
wc -c /etc/crontab
```

Lo anterior devolverá que el tamaño del archivo /etc/crontab es de cierto número de bytes.

Utilice el mandato **cat** para ver el contenido del archivo **/etc/crontab**, ejecutando lo siguiente:

```
cat /etc/crontab
```

Lo anterior devolverá algo similar a lo siguiente:

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/

# For details see man 4 crontabs

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  *  command to be executed
```

Para mostrar sólo las lineas que contengan la cadena de carácteres **root**, se utiliza el mandato grep como subrutina del siguiente modo:

```
cat /etc/crontab | grep root
```

Lo anterior devolverá algo similar a lo siguiente:

```
MAILTO=root
```

Para hacer lo contrario y sólo visualizar las líneas que sin la cadena de carácteres **root**, se utiliza el mandato **grep** como subrutina. Ejecute lo siguiente:

```
cat /etc/crontab | grep -v "root"
```

Lo anterior devolverá una salida similar a la siguiente:

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
HOME=/

# For details see man 4 crontabs

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  *  command to be executed
```

Lo anterior incluye también las lineas vacías. Para mostrar el mismo resultado sin líneas vacías, se utiliza el mismo mandato ejecutando como subrutina el mandato **sed** con la opción **-e** (ejecutar) y **'/^$/d'** como argumentos, donde **sed** es un editor para filtrado y transformación de texto y **/^$/d** se refiere a líneas vacías:

```
cat /etc/crontab | grep -v "root" | sed -e '/^$/d'
```

Lo anterior devolverá una salida similar a la siguiente:

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
HOME=/
# For details see man 4 crontabs
# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  *  command to be executed
```

Ejecute:

```
head -3 /etc/crontab
```

El mandato **head** devolverá la siguiente salida, mostrando las 3 primeras líneas del archivo /etc/crontab.

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
```

Ejecute:

```
tail -3 /etc/crontab
```

El mandato tail devolverá la siguiente salida, mostrando las 3 últimas líneas del archivo /etc/crontab.

```
# |  |  |  |  |
# *  *  *  *  *  command to be executed
```

Ejecute:

```
sort /etc/passwd |grep 0
```

Lo anterior devolverá como la salida el contenido del archivo /etc/passwd, ordenando las líneas por nombre, pero sólo mostrando aquellas líneas que incluyen el carácter 0.

```
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
fulano:x:500:500:Fulano de Tal:/home/fulano:/bin/bash
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
halt:x:7:0:halt:/sbin:/sbin/halt
operator:x:11:0:operator:/root:/sbin/nologin
root:x:0:0:root:/root:/bin/bash
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
sync:x:5:0:sync:/sbin:/bin/sync
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
```

Ejecute:

```
sort -r /etc/passwd |grep 0
```

Lo anterior devolverá como la salida el contenido del archivo /etc/passwd, ordenando las líneas por nombre, en orden inverso, pero sólo las líneas que incluyen el carácter 0.

```
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
root:x:0:0:root:/root:/bin/bash
operator:x:11:0:operator:/root:/sbin/nologin
halt:x:7:0:halt:/sbin:/sbin/halt
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
fulano:x:500:500:Fulano de Tal:/home/fulano:/bin/bash
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
```

De los dos mandatos anteriores, observe que los datos de cada línea son delimitados por el carácter : (dos puntos). Ejecute lo siguiente:

```
cat /etc/passwd |grep 0 | cut -d ":" -f1
```

El contenido del archivo /etc/passwd es mostrado, pero sólo las líneas que incluyen el carácter 0 y mostrando sólo la primera columna de datos del archivo, definiendo el carácter : (dos puntos) como delimitador entre las columnas.

```
root
sync
shutdown
halt
uucp
operator
games
gopher
ftp
avahi
avahi-autoipd
fulano
```

Ejecute:

```
cat /etc/passwd | grep 0 | cut -d ":" -f3
```

Se muestra el contenido del archivo /etc/passwd, peor sólo las líneas que incluyen el carácter 0 y sólo mostrando la tercera columna de datos del archivo, definiendo el carácter : (dos puntos) como delimitador entre las columnas.

```
0
5
6
7
10
11
12
13
14
70
170
500
```

Ejecute:

```
sort /etc/passwd | grep 0 | cut -d ":" -f1
```

Lo anterior muestra el contenido del archivo /etc/passwd, ordenando las líneas por nombre, pero sólo aquellas que contienen el carácter 0 y sólo mostrando la primera columna de datos, considerando que se utilizó el carácter : (dos puntos) como delimitador entre las columnas.

```
avahi-autoipd
avahi
ftp
fulano
games
gopher
halt
operator
root
shutdown
sync
uucp
```

17.2.6. Enlaces físicos y simbólicos.

Existen dos tipos de enlaces hacia archivos, los físicos (o duros) y los simbólicos (o blandos). Ambos permiten economizar espacio en el sistema de archivos cuando hay circunstancias en las cuales se necesita utilizar los mismos archivos o directorios en diversos lugares.

Los enlaces físicos sólo pueden apuntar hacia archivos dentro de una misma partición. Básicamente crean inodos que apuntan a un mismo archivo, es decir, se tiene un archivo con varios nombres. Sólo es posible ver hacia qué archivo apuntan consultando el número de inodo, como sería con el mandato **ls** con la opción -i. Sólo se pueden crear enlaces físicos hacia archivos existentes. Si se borra el archivo original, éste prevalece gracias al enlace físico.

Los enlaces simbólicos pueden hacia archivos y directorios en cualquier parte del sistema de archivos, sin importar en qué partición se encuentren. Son archivos especiales con una ruta hacia un archivo o directorio. El mandato **ls** con la opción -l puede mostrar hacia dónde apunta un enlace simbólico en particular. Se pueden crear enlaces simbólicos que apunten hacia archivos o directorios inexistentes. Si se borra el archivo original, el enlace simbólico simplemente apuntará hacia un archivo o directorio inexistente.

Regrese al directorio de inicio.

```
cd
```

Genere el directorio cd ~/pruebas-enlaces y cambia hacia éste.

```
mkdir ~/pruebas-enlaces ; cd ~/pruebas-enlaces
```

Genere un enlace simbólico que apunte hacia el archivo /boot/grub/device.map:

```
ln -s /boot/grub/device.map .
```

Visualice el resultado con el mandato **ls** con la opción -l:

```
ls -l
```

La salida debe devolver algo similar a lo siguiente:

```
total 0
lrwxrwxrwx 1 fulano fulano 21 jun 21 18:10 device.map -> /boot/grub/device.map
```

Copie el archivo /etc/hosts dentro del directorio ~/pruebas-enlaces:

```
cp /etc/hosts .
```

Genere un enlace físico denominado hosts2 que apunte hacia el archivo hosts, ejecutando lo siguiente:

```
ln hosts hosts2
```

Visualice el resultado con el mandato **ls** con la opción **-l**:

```
ls -l
```

La salida debe devolver algo similar a lo siguiente:

```
total 8
lrwxrwxrwx 1 jbarrios jbarrios  21 jun 21 18:10 device.map -> /boot/grub/device.map
-rw-r--r-- 2 jbarrios jbarrios 115 jun 21 18:13 hosts
-rw-r--r-- 2 jbarrios jbarrios 115 jun 21 18:13 hosts2
```

Note que en la segunda columna, la correspondiente al número de inodos utilizados, hay un número 2 para los archivos hosts y hosts2.

Para cotejar que efectivamente los inodos correspondientes de los archivos hosts y hosts2 tienen el mismo número, ejecute el mandato **ls** con la opción -i:

```
ls -i
```

La salida debe devolver algo similar a lo siguiente:

```
4980841 device.map  4980842 hosts  4980842 hosts2
```

Borre el archivo hosts.

```
rm hosts
```

Verifique que el archivo hosts ha desaparecido y que el archivo hosts2 permanece intacto.

```
ls -l
```

La salida debe devolver algo similar a lo siguiente:

```
total 4
lrwxrwxrwx 1 jbarrios jbarrios  21 jun 21 18:10 device.map -> /boot/grub/device.map
-rw-r--r-- 1 jbarrios jbarrios 115 jun 21 18:13 hosts2
```

También se pueden generar enlaces simbólicos utilizando el mandato cp con la opción -s, del siguiente modo:

```
cp -s hosts2 hosts
```

Visualice el resultado con el mandato **ls** con la opción -l:

```
ls -l
```

La salida debe devolver algo similar a lo siguiente:

```
total 8
lrwxrwxrwx 1 jbarrios jbarrios  21 jun 21 18:10 device.map -> /boot/grub/device.map
lrwxrwxrwx 1 jbarrios jbarrios   6 jun 21 18:28 hosts -> hosts2
-rw-r--r-- 1 jbarrios jbarrios 115 jun 21 18:13 hosts2
```

17.2.7. Bucles.

Regrese al directorio de inicio.

```
cd
```

Ejecute lo siguiente, donde se utiliza el mandato **perl** ejecutando (**-e**) el guión for($i=1;$i<10;$i++){print "$i\n";}, en el cual se genera la variable **i** que es igual a 1 y menor a 10 y a la cual se va sumando y devuelve una salida con el valor de **i con retorno de carro**.

```
perl -e 'for($i=1;$i<10;$i++){print "$i\n";}'
```

Lo anterior devolverá una salida similar a la siguiente:

```
1
2
3
4
5
6
7
8
9
```

Modifique el guión del mandato anterior y reemplace **"$i\n"** por **"Número $i\n"** del siguiente modo:

```
perl -e 'for($i=1;$i<10;$i++){print "Número $i\n";}'
```

Lo anterior devolverá una salida similar a la siguiente:

```
Número 1
Número 2
Número 3
Número 4
Número 5
Número 6
Número 7
Número 8
Número 9
```

Para la salida en un archivo, añada al mandato anterior >> ~/texto.txt, lo cual redirigirá la salida hacia el archivo ~/texto.txt:

```
perl -e 'for($i=1;$i<10;$i++){print "Número $i\n";}' >> ~/texto.txt
```

Lo anterior sólo devolverá el símbolo de sistema. Utilice el mandato **cat** para visualizar el contenido del archivo ~/texto.txt:

```
cat ~/texto.txt
```

Lo anterior devolverá una salida similar a la siguiente y que corresponde al contenido del archivo ~/texto.txt:

```
Número 1
Número 2
Número 3
Número 4
Número 5
Número 6
Número 7
Número 8
Número 9
```

Para hacer lo mismo que hizo con el mandato **perl**, pero utilizando el mandato **bash**, ejecute lo siguiente:

```
for i in {1..9}
do
echo -e "Número $i" >> ~/texto-con-bash.txt
done
```

Lo anterior sólo regresa el símbolo de sistema. Utilice el mandato **cat** para visualizar el contenido del archivo ~/texto-con-bash.txt, ejecute lo siguiente:

```
cat ~/texto-con-bash.txt
```

Lo anterior devolverá una salida similar a la siguiente y que corresponde al contenido del archivo ~/texto-con-bash.txt:

```
Número 1
Número 2
Número 3
Número 4
Número 5
Número 6
Número 7
Número 8
Número 9
```

A continuación aprenderá a utilizar funciones más avanzadas. En el siguiente caso usted creará respaldos de un conjunto de archivos de imágenes, asignando a cada uno un nombre distinto al que tenían en su directorio de origen. Primero creará un nuevo directorio:

```
mkdir ~/respaldos
```

Ejecute los siguientes mandatos:

```
cd /usr/share/pixmaps/
for f in *.png
do
cp $f ~/respaldos/copia-$f
done
cd
```

Lo anterior hará la copia en serie de los archivos dentro de **/usr/share/pixmaps/** dentro de **~/respaldos/** anteponiendo en el nombre de las copias la palabra «copia». Para ver el contenido del directorio **~/respaldos/**, ejecute lo siguiente:

```
ls ~/respaldos/
```

Se definirán dos variables ($hombre y $mujer), creando el archivo parejas.txt y usando los datos de éste y se ejecutará una rutina por cada conjunto de variables.

```
cd
echo "Juan Ana" >> parejas.txt
echo "Pedro Eva" >> parejas.txt
echo "Pablo Gaby" >> parejas.txt
echo "Jorge Bety" >> parejas.txt
echo "Pepe Sara" >> parejas.txt
while read hombre mujer
do
echo "$hombre es pareja de $mujer"
echo "----------------------------------------"
done < parejas.txt
```

17.2.8. Aliases.

Regrese a su directorio de inicio.

```
cd
```

Ejecute:

```
touch algo-nuevo.txt
touch otro-nuevo.txt
cp algo-nuevo.txt otro-nuevo.txt
```

Lo anterior creo los archivos **algo-nuevo.txt** y **otro-nuevo.txt** y se creó una copia de **algo-nuevo.txt**, sobre escribiendo, sin diálogo para confirmar, al archivo **otro-nuevo.txt**.

Ejecute:

```
alias cp="cp -i"
cp algo-nuevo.txt otro-nuevo.txt
```

Lo anterior creó un alias denominado **cp**, el cual corresponde al mandato **cp** con la opción **-i** (cp en modo interactivo), lo cual hace que se muestre un diálogo de confirmación antes de sobre-escribir un archivo.

Para eliminar este alias, ejecute lo siguiente:

```
unalias cp
```

Ejecute lo siguiente para crear **alias personalizado**, denominado **mandatopersonal**:

```
alias mandatopersonal="ls -l |less"
```

Lo anterior crea un **alias** que consiste en ejecutar el mandato **ls** con la opción -l y que además ejecutará como subrutina al mandato **less**. Ejecute **mandatopersonal**.

```
mandatopersonal /etc
```

Lo anterior debe haber mostrado el contenido del directorio **/etc**, utilizando **less** para poder desplazar la pantalla. Para salir de **less**, pulse la tecla **q**.

Los aliases creados perduran hasta que es cerrada la sesión del usuario. Para que cualquier alias sea permanente para un usuario en particular, hay que especificar éstos dentro del archivo **~/.bashrc** (CentOS, Fedora y Red Hat Enterprise Linux) o bien dentro del archivo **~/.aliases** (SUSE Linux Enterprise y openSUSE).

Para ver la lista de aliases predeterminados del sistema, sólo ejecute el mandato **alias**.

```
alias
```

17.2.9. Apagado y reinicio de sistema.

Para que el sistema finalice apropiadamente todos los servicios en ejecución, guarde en disco las consignaciones pendientes y desmonte de forma segura todos los sistemas de archivos, utilice los mandatos **reboot** o bien **poweroff**.

Para reiniciar el sistema de inmediato, ejecute el mandato **reboot**:

```
reboot
```

El mandato **reboot** puede ser utilizado por usuarios regulares y su uso es controlado a través de **PAM**.

Si requiere hacer un reinicio del sistema, con un lapso de tiempo y un aviso a los usuarios que estén conectados al sistema, utiliza el mandato **shutdown** con la opción **-r** y el número de minutos que quiera dar de tiempo antes de realizar el proceso de reinicio. En el siguiente ejemplo, el proceso de reinicio del sistema se realizará dentro de 5 minutos:

```
shutdown -r 5
```

Si utiliza el mandato **shutdown** con la opción **-r**, sin más argumentos, de modo predeterminado el sistema reiniciará en un minuto, enviando un mensaje de advertencia a todos los usuarios conectados al sistema.

El mandato **shutdown** sólo puede ser utilizado por el usuario root.

Para apagar el sistema de inmediato, ejecute el mandato **poweroff**:

```
poweroff
```

Al igual que el mandato **reboot**, el mandato **poweroff** puede ser utilizado por usuarios regulares y su uso es controlado a través de **PAM**.

Si requiere hacer un apagado del sistema, con un lapso de tiempo y un aviso a los usuarios que estén conectados al sistema, utiliza el mandato **shutdown** con la opción **-h** y el número de minutos que quiera dar de tiempo antes de realizar el proceso de apagado. En el siguiente ejemplo, el proceso de apagado del sistema se realizará dentro de 5 minutos:

```
shutdown -h 5
```

Si utiliza el mandato **shutdown** con la opción **-h**, sin más argumentos, de modo predeterminado el sistema se apagará en un minuto, enviando un mensaje de advertencia a todos los usuarios conectados al sistema.

Para cancelar el procesos de apagado o reinicio del sistema, se utiliza el mandato **shutdown** con la opción **-c**.

```
shutdown -c
```

Recuerde que el mandato **shutdown** sólo puede ser utilizado por el usuario root.

Continúe con el documento titulado «Compresión y descompresión de archivos.»

18. Compresión y descompresión de archivos.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales (incluyendo su publicación, a través de cualquier medio, por entidades con fines de lucro). c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en castellano. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

18.1. Introducción.

Por favor, **siga los procedimientos al pie de la letra**. En varios ejemplos utilizará el carácter ~ (tilde), que es una forma de abreviar el directorio de inicio del usuario utilizado.

18.1.1. Acerca de ZIP.

ZIP es un formato de archivo simple, creado originalmente por Phil Katz, fundador de PKWARE, el cual comprime cada uno de los archivos que contiene de forma separada, lo cual permite recuperar cada uno de los archvios almacenados sin tener que leer el resto del archivo ZIP que los contiene, lo que permite un mejor rendimiento. Cada archivo puede ser almacenado sin compresión o con una amplia variedad de algoritmos de compresión, aunque el más utilizado y práctico es el algoritmo original de Phil Katz.

18.1.2. Acerca de TAR.

El **formato de almacenamiento** de archivos conocido como TAR o **T**ape **AR**chiver (archivador en cinta), fue diseñado para el almacenamiento de archivos en cintas magnéticas. El formato se procesa de manera lineal, de modo que es necesario recorrer todo el archivo para poder poder extraer cualquier elemento que éste contenido en el archivo TAR. Actualmente está definido en los estándares POSIX.1-1998 y POSIX.1-2001

18.1.3. Acerca de GZIP.

El **formato de compresión** GZIP (GNU ZIP), creado por Mark Adler y Jean-loup Gailly, es una alternativa a los formatos LZW y otros algoritmos patentados que limitaban el uso del programa **compress**, hasta entonces lo más comúnmente utilizado en Unix. GZIP utiliza la biblioteca Zlib, la cual se basa sobre el algoritmo Deflate, que es una combinación del LZ77 y la codificación Huffman. Es importante señalar que GZIP sólo realiza la compresión de los archivos, el almacenamiento se realiza utilizando TAR o cualquier otro **formato de almacenamiento** de archivos.

18.1.4. Acerca de BZIP2

El **formato de compresión** BZIP2, desarrollado y mantenido por Julian Seward, utiliza los algoritmos de compresión de Burrows-Wheeler y el algoritmo de codificación de Huffman. Aunque el porcentaje de compresión de los archivos depende del contenido de éstos mismos, resulta una mejor alternativa a ZIP y GZIP, pero con un mayor consumo de memoria y recursos de sistema.

18.1.5. Acerca de XZ.

El **formato de compresión** XZ, creado y mantenido por Lasse Collin, utiliza el algoritmo de compresión LZMA2, a través de la biblioteca liblzma. Tiene un mejor rendimiento que BZIP2 (consume menos memoria y recursos de sistema) con mejores tasas de compresión. Es el formato utilizado hoy en día para la compresión de archivos TAR de códigos fuente, aunque GZIP aún es el formato más utilizado a la fecha para distribución de código fuente de Software Libre.

18.2. Procedimientos.

Ingrese al sistema como el usuario **root** y asegúrese que estén instalados los paquetes tar, zip, unzip, gzip, bzip2 y xz.

Si utiliza **CentOS**, **Fedora™** o **Red Hat™ Enterprise Linux**, ejecute lo siguiente:

```
yum -y install tar zip unzip gzip bzip2 xz
```

Si utiliza **openSUSE™** o **SUSE™ Linux Enterprise**, ejecute lo siguiente:

```
yast -i tar zip unzip gzip bzip2 xz
```

Al terminar, cierre la sesión del usuario **root**, ejecutando el mandato **exit**:

```
exit
```

18.2.1. Preparativos.

Ingrese nuevamente al sistema como usuario regular (fulano).

A fin de disponer de datos con los cuales experimentar, copie el directorio **/usr/share/pixmaps** dentro del directorio de inicio del usuario utilizado.

```
cp -a /usr/share/pixmaps ~/
```

18.2.2. Compresión y descompresión de archivos *.zip.

Consulte el manual del mandato **zip** ejecutando lo siguiente:

```
man 1 zip
```

Consulte el manual del mandato **unzip** ejecutando lo siguiente:

```
man 1 unzip
```

Genere un archivo .zip ejecutando lo siguiente:

```
zip -r foo.zip pixmaps/
```

Para mostrar la lista del contenido del archivo **foo.zip**, ejecute:

```
unzip -l foo.zip
```

Extraiga el contenido del archivo **foo.zip** dentro del directorio **~/ejemplos1/**, ejecutando lo siguiente:

```
unzip foo.zip -d ~/ejemplos1/
```

Si la salida le pregunta si desea sobre-escribir los archivos existentes, responda que si a todo pulsando la letra **A** (sobre-escriir todo) y la tecla **ENTER**.

Extraiga el contenido del archivo **foo.zip** dentro del directorio **~/ejemplos1/**, pero sólo extrayendo los archivos del primer nivel con extensión *.png, ejecutando lo siguiente:

```
unzip foo.zip -d ~/ejemplos1/ *.png
```

Si la salida le pregunta si desea sobre-escribir los archivos existentes, responda que si a todo pulsando la letra **A** (sobre-escriir todo) y la tecla **ENTER**.

Extraiga el contenido del archivo **foo.zip** dentro del directorio **~/ejemplos1/**, pero sólo extrayendo los archivos del segundo nivel con extensión *.png, ejecutando lo siguiente:

```
unzip foo.zip -d ~/ejemplos1/ */*.png
```

Si la salida le pregunta si desea sobre-escribir los archivos existentes, responda que si a todo pulsando la letra **A** (sobre-escriir todo) y la tecla **ENTER**.

18.2.3. Creación y extracción de archivos *.tar.

Consulte el manual del mandato **tar** ejecutando lo siguiente:

```
man 1 tar
```

Genere un archivo .tar (sin compresión) ejecutando lo siguiente:

```
tar cf foo.tar pixmaps/
```

Para mostrar la lista del contenido del archivo **foo.tar**, ejecute:

```
tar tvf foo.tar
```

Extraiga el contenido del archivo **foo.tar** dentro del directorio **~/ejemplos1/**, ejecutando lo siguiente:

```
tar xvf foo.tar -C ~/ejemplos1/
```

Extraiga el contenido del archivo **foo.tar** dentro del directorio **~/ejemplos1/**, pero sólo extrayendo los archivos con extensión *.png, ejecutando lo siguiente:

```
tar xvf foo.tar -C ~/ejemplos1/ --wildcards '*.png'
```

18.2.4. Compresión y descompresión de archivos *.tar.gz.

Genere un archivo .tar.gz (con compresión GZIP) ejecutando lo siguiente:

```
tar zcf foo.tar.gz pixmaps/
```

Para mostrar la lista del contenido del archivo **foo.tar.gz**, ejecute:

```
tar ztvf foo.tar.gz
```

Extraiga el contenido del archivo **foo.tar.gz** dentro del directorio **~/ejemplos1/** ejecutando lo siguiente:

```
tar zxvf foo.tar.gz -C ~/ejemplos1/
```

Extraiga el contenido del archivo **foo.tar.gz** dentro del directorio **~/ejemplos1/**, pero sólo extrayendo los archivos con extensión *.png, ejecutando lo siguiente:

```
tar zxvf foo.tar.gz -C ~/ejemplos1/ --wildcards '*.png'
```

18.2.5. Compresión y descompresión de archivos *.tar.bz2.

Genere un archivo .tar.bz2 (con compresión BZip2) ejecutando lo siguiente:

```
tar jcf foo.tar.bz2 pixmaps/
```

Para mostrar la lista del contenido del archivo **foo.tar.bz2**, ejecute:

```
tar jtvf foo.tar.bz2
```

Extraiga el contenido del archivo **foo.tar.bz2** dentro del directorio **~/ejemplos1/**, ejecutando lo siguiente:

```
tar jxvf foo.tar.bz2 -C ~/ejemplos1/
```

Extraiga el contenido del archivo **foo.tar.bz2** dentro del directorio **~/ejemplos1/**, pero sólo extrayendo los archivos con extensión *.png, ejecutando lo siguiente:

```
tar jxvf foo.tar.bz2 -C ~/ejemplos1/ --wildcards '*.png'
```

18.2.6. Compresión y descompresión de archivos *.tar.xz.

Genere un archivo .tar.xz (con compresión XZ) ejecutando lo siguiente:

```
tar Jcf foo.tar.xz pixmaps/
```

Para mostrar la lista del contenido del archivo **foo.tar.xz**, ejecute:

```
tar Jtvf foo.tar.xz
```

Extraiga el contenido del archivo **foo.tar.xz** dentro del directorio **~/ejemplos1/**, ejecutando lo siguiente:

```
tar Jxvf foo.tar.xz -C ~/ejemplos1/
```

Extraiga el contenido del archivo **foo.tar.xz** dentro del directorio **~/ejemplos1/**, pero sólo extrayendo los archivos con extensión *.png, ejecutando lo siguiente:

```
tar Jxvf foo.tar.xz -C ~/ejemplos1/ --wildcards '*.png'
```

18.2.7. Crear respaldos del sistema de archivos.

Por lo general los respaldos se hacen sin compresión, a fin de que sean rápidos y consuman la menor cantidad de recursos de sistema posibles y sólo se utiliza compresión cuando se tiene un espacio muy limitado en el sistema de archivo, unidades de cinta u otras unidades de almacenamiento.

Hay tres tipos de respaldos:

- **Completos:** Se consideran de **nivel 0**.
- **Diferenciales**: Se consideran de **nivel 1**. Consisten en respaldos que dependen de un respaldo completo para poder restaurar todos los datos, sólo archivando los archivos nuevos o que cambiaron respecto del último respaldo completo. Es decir, para restaurar los datos se requiere el último respaldo completo y el respaldo diferencial. Hoy en día se utilizan muy poco, salvo que el administrador del sistema sea poco experimentado o bien porque así es como lo prefiere, pues consumen mucho más espacio en el sistema de archivos que los respaldos incrementales.
- **Incrementales**: Se consideran de **nivel 1** cuando hay un solo respaldo completo antes de éste, de **nivel 2** cuando hay un respaldo completo y un respaldo incremental antes de éste, de **nivel 3** cuando hay un respaldo completo y dos incrementales antes de éste y así sucesivamente. Son similares al respaldo diferencial, pero éstos pueden hacerse a partir de un respaldo completo y/o un diferencial y/o otros incrementales, restaurando los datos en secuencia, por lo cual permiten ahorrar el espacio disponible en el sistema de archivos. Es decir, para restaurar los datos, se requiere el último respaldo completo y uno o más respaldos incrementales.

Un respaldo completo se puede realizar con el mandato **tar**, con las opciones cpf (crear archivo, preservar permisos, definir nombre del archivo), el nombre del archivo *.tar a crear, la opción **-g** (definir crear un archivo incremental en el nuevo formato de GNU) y el nombre del archivo con extensión ***.snar** (que proviene de la contracción de ***sn****apshot* ***ar****chive*). Éste último es utilizado por el mandato **tar** para almacenar la información respecto de qué fue lo que se respaldó. La opción **p** es importante para crear y restaurar los respaldos, pues permite preservar los permisos y atributos originales de los datos. Si se omite esta opción, todo el contenido almacenado y restaurado sería propiedad del usuario root.

Cambie al usuario root. A partir de este paso sólo podrá realizar los procedimientos con privilegios de root.

```
su -l
```

Genere el directorio **/var/respaldos** ejecutando lo siguiente:

```
mkdir /var/respaldos
```

En el siguiente ejemplo se creará un respaldo completo del directorio /home, guardando los archivos de datos e incremental dentro de /var/respaldos.

```
tar cpf /var/respaldos/completo.tar \
    -g /var/respaldos/registro.snar /home
```

Para crear un respaldo incremental, solo se define el nombre de un nuevo archivo, utilizando el mismo archivo *.snar.

```
tar cpf /var/respaldos/incremental-1.tar \
    -g /var/respaldos/registro.snar /home
```

Para crear un segundo respaldo incremental, se ejecutaría lo siguiente:

```
tar cpf /var/respaldos/incremental-2.tar \
    -g /var/respaldos/registro.snar /home
```

Para crear un tercer respaldo incremental, se ejecutaría lo siguiente:

```
tar cpf /var/respaldos/incremental-3.tar \
    -g /var/respaldos/registro.snar /home
```

Para restaurar los datos, se ejecutaría lo siguiente:

```
tar xpf /var/respaldos/completo.tar \
    -g /var/respaldos/registro.snar -C /
tar xpf /var/respaldos/incremental-1.tar \
    -g /var/respaldos/registro.snar -C /
tar xpf /var/respaldos/incremental-2.tar \
    -g /var/respaldos/registro.snar -C /
tar xpf /var/respaldos/incremental-3.tar \
    -g /var/respaldos/registro.snar -C /
```

Los respaldos también se pueden hacer en múltiples volúmenes cuando el espacio en las unidades de almacenamiento es limitado. Se hacen de modo similar a los respaldos completos, pero añadiendo la opción **-M**, para indicar que se realizará en múltiples volúmenes y la opción **-L**, para indicar el tamaño del volumen en bytes.

En el siguiente ejemplo se creará un respaldo de /home en una unidad de almacenamiento externa, en cuatro partes de 4 GiB (4194304 bytes) cada una, **asumiendo** que /home ocupa menos de 16 GiB (16777216 bytes) de espacio en el sistema de archivos y que la unidad de almacenamiento externo está montada en el directorio **/media/DISCO/**:

```
tar cpf /media/DISCO/parte01.tar \
    -g /media/DISCO/registro.snar -M -L 4194304 /home
tar cpf /media/DISCO/parte02.tar \
    -g /media/DISCO/registro.snar -M -L 4194304 /home
tar cpf /media/DISCO/parte03.tar \
    -g /media/DISCO/registro.snar -M -L 4194304 /home
tar cpf /media/DISCO/parte04.tar \
    -g /media/DISCO/registro.snar -M -L 4194304 /home
```

La restauración de los datos se hace de modo similar a la de los respaldos incrementales, pero añadiendo la opción **-M** para indicar que se trata de un respaldo de varios volúmenes.

```
tar xpf /media/DISCO/parte01.tar \
    -g /media/DISCO/registro.snar -M -C /
tar xpf /media/DISCO/parte02.tar \
    -g /media/DISCO/registro.snar -M -C /
tar xpf /media/DISCO/parte03.tar \
    -g /media/DISCO/registro.snar -M -C /
tar xpf /media/DISCO/parte04.tar \
    -g /media/DISCO/registro.snar -M -L -C /
```

Al terminar los procedimientos, cierre la sesión de root.

```
exit
```

Continúe con el documento titulado «Gestión de procesos y trabajos.»

19. Gestión de procesos y trabajos.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales (incluyendo su publicación, a través de cualquier medio, por entidades con fines de lucro). c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en castellano. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

19.1. Introducción.

En este documento aprenderá el uso de los mandatos jobs, bg, fg, kill, killall, ps, top y taskset.

Un **PID** o identidad de proceso, es un decimal entero que especifica un proceso o un grupo de procesos. Todos los procesos que se ejecuten en un sistema pueden ser terminados o aniquilados utilizando el mandato **kill** o bien el mandato **killall**, excepto por el **proceso con PID 1**, el cual corresponde siempre a **/sbin/init**.

Un **Job ID** o identidad de trabajo, identifica un trabajo o grupo de trabajos que se ejecutan en segundo plano. El mandato **kill** solo permitirá terminar o aniquilar los trabajos originados de una misma consola o intérprete de mandatos en ejecución.

Los trabajos se gestionan a través de los mandatos bg, fg y jobs.

Los procesos se terminan normalmente con **SIGTERM** (número de señal 15) o bien se aniquilan con **SIGKILL** (número de señal 9), utilizando el mandato **kill** o el mandato **killall**.

19.2. Procedimientos.

Ingrese al sistema como **root**.

Si utiliza CentOS, Fedora™ o Red Hat™ Enterprise Linux, ejecute lo siguiente:

```
yum -y install procps top util-linux-ng
```

Si utiliza openSUSE™ o SUSE™ Linux Enterprise, ejecute lo siguiente:

```
yast -i procps psmisc util-linux
```

Cierre la sesión como root e ingrese nuevamente al sistema como usuario regular (fulano) o bien ejecute lo siguiente:

```
su -l fulano
```

19.2.1. Uso de jobs, bg y fg.

Ejecute el mandato **sleep** con el valor **600** (pausa por 600 segundos), a fin de utilizar éste como trabajo de ejemplo.

```
sleep 600
```

Pulse CTRL+Z, lo cual devolverá una salida similar a la siguiente:

```
^Z
[1]+  Detenido                sleep 600
```

Utilice el mandato **jobs** para visualizar el trabajo detenido:

```
jobs
```

Lo anterior debe devolver la siguiente salida:

```
[1]+  Detenido                sleep 600
```

Ejecute el mandato **bg** para reactivar el trabajo 1 en segundo plano:

```
bg 1
```

La salida deberá devolver lo siguiente:

```
[1]+ sleep 600 &
```

Ejecute nuevamente el mandato **sleep**, con el valor **700** y un signo *amperson* (&) al final:

```
sleep 700 &
```

La salida devolverá algo similar a lo siguiente, indicando el número de trabajo (2) y el número de identidad de proceso (PID):

```
[2] 3768
```

Con lo anterior habrá enviado este trabajo directamente a segundo plano.

Utilice el mandato **jobs** para visualizar los trabajos en segundo plano:

```
[1]-  Ejecutando              sleep 600 &
[2]+  Ejecutando              sleep 700 &
```

Para enviar a primer plano el primer trabajo, ejecute el mandato **fg** con **1** como argumento:

```
fg 1
```

Lo anterior hará que **sleep 600** regrese a primer plano.

Para terminar este último trabajo, pulse CTRL+C.

19.2.2. Uso de ps, kill y killall.

Utilice el mandato **ps**, con las opciones **aux** (todos los procesos en todas las terminales, orientado a usuarios e incluyendo todos los procesos con o sin un TTY), utilizando una tubería (|) con el mandato **less** para poder observar cómodamente la salida y los valores de las columnas USER, PID, %CPU, %MEM, VSZ, RSS, TTY, STAT, START, TIME y COMMAND.

```
ps aux |less
```

Repita el mandato anterior, esta vez utilizando una tubería (|) y el mandato **grep** para visualizar solamente los procesos cuyo nombre incluyan la cadena *sleep*:

```
ps aux |grep sleep
```

Lo anterior le devolverá una salida similar a la siguiente:

```
fulano  3768  0.0  0.0 100984   568 pts/2    S    11:50   0:00 sleep 700
fulano  3820  0.0  0.0 103396   832 pts/2    S+   11:51   0:00 grep --color=auto sleep
```

La segunda columna corresponde al número de identidad de proceso (PID), determine el correspondiente al procesos **sleep 700**.

Utilice el mandato **kill** con este número de identidad de proceso, con la finalidad terminar éste de manera normal (**SIGTERM**).

```
kill 3768
```

Lo anterior devolverá la siguiente salida:

```
[2]+  Terminado               sleep 700
```

Ejecute de nuevo el mandato **sleep**, ahora con **800** como argumento, con un signo *amperson* (&) al final, a fin de generar un nuevo trabajo en segundo plano.

```
sleep 800 &
```

Lo anterior debe devolver una salida similar a la siguiente:

```
[1] 3820
```

La forma más sencilla de terminar de manera normal (SIGTERM) un trabajo, utilizando el mandato **kill**, es utilizar éste con el número de trabajo, precedido por un signo %, como argumento. Ejecute el siguiente mandato:

```
kill %1
```

La salida solo devolverá el símbolo de sistema. Si vuelve a pulsar la tecla ENTER, la salida será similar a la siguiente:

```
[1]+  Terminado               sleep 800
```

Ejecute de nuevo el mandato **sleep**, ahora con **850** como argumento, con un signo *amperson* (&) al final, a fin de generar un nuevo trabajo en segundo plano.

```
sleep 850 &
```

Lo anterior debe devolver una salida similar a la siguiente:

```
[1] 3830
```

Utilice nuevamente el mandato **ps**, con las opciones **aux**, agregando una tubería y el mandato **grep** para visualizar en la salida solamente los procesos cuyo nombre incluyan la cadena sleep:

```
ps aux |grep sleep
```

Lo anterior le devolverá una salida similar a la siguiente:

```
fulano  3830  0.0  0.0 100984   564 pts/2    S    11:54   0:00 sleep 850
fulano  3835  0.0  0.0 103396   828 pts/2    S+   11:56   0:00 grep --color=auto sleep
```

Determine el número de identidad de proceso correspondiente al procesos **sleep 850**.

Utilice el mandato **kill** con este número de identidad de proceso, correspondiente a **sleep 850**, con la finalidad **aniquilar** éste (**SIGKILL**).

```
kill -9 3830
```

Lo anterior debe devolver la siguiente salida:

```
[1]+  Terminado (killed)      sleep 850
```

Ejecute lo siguiente para generar dos nuevos trabajos en segundo plano:

```
sleep 600 & sleep 700 &
```

Lo anterior devolverá algo similar a lo siguiente:

```
[1] 3924
[2] 3925
```

Utilice el mandato **jobs** para visualizar ambos trabajos:

```
jobs
```

Lo anterior deberá devolver la siguiente salida:

```
[1]-  Ejecutando              sleep 600 &
[2]+  Ejecutando              sleep 700 &
```

Utilice el mandato **ps**, con la opción **-j**, para visualizar los números de identidad de proceso (PID) de estos trabajos:

```
ps -j
```

Lo anterior debe devolver una salida similar a la siguiente:

```
  PID  PGID   SID TTY          TIME CMD
 3624  3624  3624 pts/2    00:00:00 bash
 3924  3924  3624 pts/2    00:00:00 sleep
 3925  3925  3624 pts/2    00:00:00 sleep
 3937  3937  3624 pts/2    00:00:00 ps
```

Utilice el mandato **killall** con la cadena «**sleep**» como argumento, a fin de **terminar** de manera normal de todos los procesos denominados *sleep*.

```
killall sleep
```

Lo anterior deberá devolver la siguiente salida:

```
[1]-  Terminado              sleep 600
[2]+  Terminado              sleep 700
```

Ejecute lo siguiente para generar dos nuevos trabajos en segundo plano:

```
sleep 800 & sleep 900 &
```

Lo anterior devolverá algo similar a lo siguiente:

```
[1] 3949
[2] 3950
```

Utilice el mandato **jobs** para visualizar ambos trabajos:

```
jobs
```

Lo anterior deberá devolver la siguiente salida:

```
[1]-  Ejecutando             sleep 800 &
[2]+  Ejecutando             sleep 900 &
```

Utilice el mandato **ps**, con la opción **-j**, para visualizar lo números de identidad de proceso (PID) de estos trabajos:

```
ps -j
```

Lo anterior debe devolver una salida similar a la siguiente:

```
  PID  PGID   SID TTY          TIME CMD
 3624  3624  3624 pts/2    00:00:00 bash
 3949  3949  3624 pts/2    00:00:00 sleep
 3950  3950  3624 pts/2    00:00:00 sleep
 3956  3956  3624 pts/2    00:00:00 ps
```

Utilice el mandato **killall**, con la opción **-s** y el valor **9**, junto con la cadena «**sleep**» como argumento, a fin de **aniquilar** (terminación anormal) de todos los procesos denominados *sleep*.

```
killall -s 9 sleep
```

Lo anterior deberá devolver la siguiente salida:

```
[1]-  Terminado (killed)      sleep 800
[2]+  Terminado (killed)      sleep 900
```

19.2.3. Uso de nice y renice.

Ejecute el mandato tar con las opciones jcf para generar el archivo pixmaps.tar.bz2 con el contenido del directorio /lib/modules, ejecutando lo siguiente:

```
tar jcf modulos.tar.bz2 /lib/modules
```

Al terminar (luego de unos minutos), utilice el mandato time para cuantificar la ejecución del mandato **tar**, con las opciones **jxf**, para descomprimir el archivo modulos.tar.bz2. El objetivo será cuantificar la descompresión con la prioridad de planificación 0 (valor predeterminado del sistema), la cual permite utilizar los recursos que regularmente permite utilizar el sistema al usuario.

```
time tar jxf modulos.tar.bz2
```

La salida debe devolver algo similar a lo siguiente:

```
real    0m13.237s
user    0m12.491s
sys     0m1.824s
```

Del mismo modo con el mandato time, utilice el mandato **nice** para ejecutar el mandato **tar**, con las opciones **jxf**, para descomprimir el archivo modulos.tar.bz2. El objetivo será realizar la descompresión cambiando la prioridad de planificación a 10 (valor predeterminado del mandato **nice** si es utilizado sin más argumentos), a fin de utilizar menos recursos de sistema.

```
time nice -n +10 tar jxf modulos.tar.bz2
```

La salida debe devolver algo similar a lo siguiente.

```
real    0m13.638s
user    0m12.947s
sys     0m1.908s
```

Los resultados deberán ser ligeramente mayores que la ejecución del mismo mandato con el valor predeterminado de prioridad de planificación (0).

Del mismo modo, utilice ahora el mandato **nice**, con la opción **-n** y el valor **19**, para ejecutar el mandato **tar**, con las opciones **jxf**, con la menor prioridad posible, para descomprimir el archivo modulos.tar.bz2. El objetivo será realizar la descompresión cambiando la prioridad de planificación a 10 (valor predeterminado del mandato **nice**), a fin de utilizar menos recursos de sistema.

```
time nice -n +20 tar jxf modulos.tar.bz2
```

La salida debe devolver algo similar a lo siguiente.

```
real    0m13.918s
user    0m13.045s
sys     0m1.875s
```

Los resultados deberán ser sensiblemente mayores que la ejecución del mismo mandato con el valor predeterminado de prioridad de planificación (0).

El usuario regular solo pude definir valores de prioridad de planificación del **0** al **19**, prioridad de planificación predeterminada a prioridad de planificación menos favorable. Los valores negativos, del **-1** al **-20**, que son los más favorables, sólo los pude utilizar **root**.

Utilizando el mandato **su**, con la opción **-c**, con la cual se indicará entre comillas un mandato a ejecutar como **root**, repita el mandato anterior, pero con valor **-20** para el mandato **nice**.

```
su -c "time nice -n -20  tar jxf modulos.tar.bz2"
```

Lo anterior solicitará se ingrese la clave de acceso de root y devolverá una salida similar a la siguiente:

```
real    0m13.328s
user    0m12.834s
sys     0m1.978s
```

Los resultados deberán ser sensiblemente inferiores que la ejecución del mismo mandato con el valor predeterminado de prioridad de planificación (0).

Para cambiar la prioridad de planificación de un proceso en ejecución, se utiliza el mandato **renice**, mismo que permite cambiar la prioridad planificada por número de procesos, usuario y grupo. Los valores de prioridad de planificación se pueden visualizar utilizando el mandato **ps**, con las opciones **alx** (todos los procesos en todas las terminales, en formato largo e incluyendo todos los procesos con o sin un TTY, respectivamente). Ejecute el siguiente mandato:

```
ps alx |less
```

Lo anterior mostrará las columnas F, UID, PID, PPID, PRI, NI, VSZ, RSS, WCHAN, STAT, TTY, TIME y COMMAND. Los valores de prioridad planificada corresponden a la sexta columna (NI).

El siguiente ejemplo cambia la prioridad de planificación a **-10** al proceso 45678:

```
su -c "renice -n -10 -p 45678"
```

El siguiente ejemplo cambia la prioridad de planificación a **-10** a todos los procesos del usuario fulano:

```
su -c "renice -n -10 -u fulano"
```

El siguiente ejemplo cambia la prioridad de planificación a **-10** a todos los procesos del grupo desarrollo:

```
su -c "renice -n -10 -g desarrollo"
```

El siguiente ejemplo cambia la prioridad de planificación a **-10** al procesos 34567 del usuario fulano:

```
su -c "renice -n -10 -p 34567 -u fulano"
```

19.2.4. Uso del mandato taskset.

Este mandato sólo tiene sentido utilizarlo cuando se dispone de más de un CPU lógico en el sistema. Ejecute el mandato **nproc** para determinar el número de CPUs lógicos en el sistema:

```
nproc
```

Lo anterior sólo devolverá el número de CPUs lógicos del sistema.

Para obtener información más detallada, ejecute el mandato **lscpu**:

```
lscpu
```

Asumiendo que el sistema dispone de dos núcleos lógicos, lo anterior puede devolver una salida similar a la siguiente:

```
Architecture:          i686
CPU op-mode(s):        32-bit
Byte Order:            Little Endian
CPU(s):                2
On-line CPU(s) list:   0,1
Thread(s) per core:    1
Core(s) per socket:    2
Socket(s):             1
Vendor ID:             GenuineIntel
CPU family:            6
Model:                 14
Stepping:              12
CPU MHz:               1200.000
BogoMIPS:              3200.10
L1d cache:             32K
L1i cache:             32K
L2 cache:              1024K
```

Lo anterior representa un resumen del contenido del archivo **/proc/cpuinfo**, que también puede consultarse ejecutando lo siguiente:

```
less /proc/cpuinfo
```

El mandato **taskset** es utilizado para establecer u obtener la afinidad de CPU de un proceso a través de su PID o bien para ejecutar un nuevo mandato con una afinidad de CPU arbitraria. La afinidad de CPU es una propiedad de planificador del núcleo de Linux que vincula un procesos a un conjunto de CPUs en el sistema. Este planificador se encargará de que se mantenga la afinidad de CPU y que el proceso sólo se ejecute en el CPU o en los CPUs especificados. Cabe señalar que de manera nativa el planificador del núcleo de Linux incluye soporte para afinidad natural, la cual consiste en que el planificador intentará mantener los procesos en el mismo CPU tanto como sea práctico para mantener un buen desempeño en el sistema, por lo cual la manipulación de la afinidad de CPU sólo es útil para ciertas tareas y aplicaciones.

Si se especifica una máscara de bit incorrecta o bien un CPU inexistente, invariablemente el mandato **taskset** devolverá un error.

La afinidad de CPU se representa a través de una máscara de bit (*bitmask*), donde el bit de menor valor corresponde al primer CPU lógico y el bit mayor corresponde al último CPU lógico. Las máscaras de bit se representan en hexadecimal:

0x00000001

Corresponde al CPU #0

0x00000002

Corresponde al CPU #1

0x00000003

Corresponde los CPUs #0 y #1

0xFFFFFFFF

Corresponde a todos los CPUs (#0 hasta #31)

Para iniciar un nuevo proceso con una afinidad de CPU en particular, se utiliza la siguiente sintaxis:

```
taskset mascara mandato
```

Ejemplo:

```
taskset 0x00000001 tar jcf modulos.tar.bz2 /lib
```

Para obtener la afinidad de CPU de un procesos en ejecución, se ejecuta el mandato **taskset** con la opción **-p** para indicar que se utilizará un PID existente y el número de PID como argumentos.

```
taskset -p pid
```

Ejemplo:

```
taskset -p 34567
```

Para cambiar la afinidad de CPU de un procesos en ejecución, se ejecuta el mandato **taskset** con la opción **-p** para indicar que se utilizará un PID existente, la mascara de afinidad de CPU deseada y el número de PID como argumentos.

```
taskset -p mascara pid
```

Ejemplo:

```
taskset -p 0x00000001 34567
```

Si se dificulta el uso de máscaras de bit en hexadecimal, también es posible utilizar la opción **-c** y una lista numérica de CPUs lógicos, donde 0 corresponde al primer CPU, 1 corresponde al segundo CPU lógico, 2 corresponde al tercer CPU lógico y así sucesivamente.

```
taskset -c -p lista pid
```

Ejemplo:

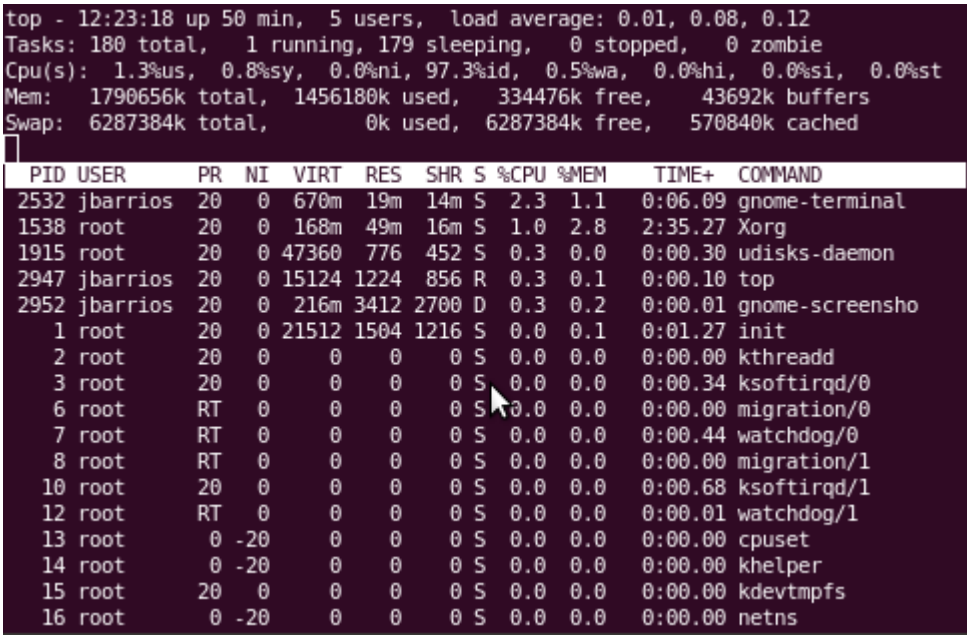
```
taskset -c -p 1 34567
```

También es posible especificar varios CPU de manera simultánea, definiendo una lista de éstos separada por comas y que también permite definir rangos. Ejemplos:

```
taskset -c 0,1 tar jcf modulos.tar.bz2 /lib
taskset -c -p 0,2 34567
taskset -c -p 4-7 34567
```

19.2.5. Uso del mandato top.

Top es una herramienta que proporciona una visualización continua y en tiempo real de los procesos activos en un sistema, como una lista que de modo predeterminado lo hace de acuerdo al uso del CPU. Puede ordenar la lista por uso de memoria y tiempo de ejecución.



Para ordenar la lista de procesos por orden de uso de memoria, pulse **SHIFT+M**. Para ordena la lista de procesos por orden de tiempo de ejecución, pulse **SHIFT+T**. Para invertir el orden de la lista, pulse **SHIFT+R**. Para activar o bien desactivar, la visualización por hilos, pulse **SHIFT+H**. Para ordenar de nuevo la lista de procesos por orden de uso de CPU, pulse **SHIFT+P**.

Para mostrar los procesos de un usuario en específico, pulse la tecla **u** y defina a continuación el nombre del usuario.

Para terminar o aniquilar cualquier proceso, pulse la tecla **k** y defina a continuación el número de identidad de proceso que corresponda y luego la señal a utilizar (9 o 15).

Para cambiar la prioridad de planificación de cualquier proceso, pulse la tecla **r** y a continuación defina el número de identidad de proceso que corresponda y luego el valor de prioridad de planificación deseado.

Para ver el la ayuda completa del mandato top, pulse la tecla **h**.

20. Uso del mandato lsof

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales (incluyendo su publicación, a través de cualquier medio, por entidades con fines de lucro). c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en castellano. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

20.1. Introducción.

20.1.1. Acerca de lsof.

Lsof significa *«listar archivos abiertos»* (**l**i**s**t open **f**iles). Es utilizado ampliamente en sistemas operativos tipo **POSIX** para hacer reportes de archivos y los procesos que están utilizando a éstos. Se puede utilizar para revisar que procesos están haciendo uso de directorios, archivos ordinarios, tuberías (*pipes*), zócalos de red (*sockets*) y dispositivos. Uno de los principales usos de determinar que procesos están haciendo uso de archivos en una partición cuando esta no se puede desmontar. **Lsof** fue desarrollado por **Vic Abell**, quien alguna vez fue director del Centro de Cómputo de la **Universidad de Purdue**.

20.2. Equipamiento lógico necesario.

20.2.1. En CentOS, Fedora™ y Red Hat™ Enterprise Linux.

Para instalar **lsof**, ejecute lo siguiente:

```
yum -y install lsof
```

20.2.2. En openSUSE™ y SUSE™ Linux Enterprise.

Para instalar **lsof**, ejecute lo siguiente:

```
yast -i lsof
```

20.3. Procedimientos.

El manual completo del mandato **lsof** puede consultarse ejecutando lo siguiente:

```
man 8 lsof
```

Para ver todos los procesos que utilizan el sistema de archivos en general, ejecute el mandato **lsof** sin opciones u argumentos:

```
lsof
```

En ejemplo de la salida típica sería como la siguiente:

```
COMMAND     PID      USER   FD      TYPE     DEVICE       SIZE       NODE NAME
init          1      root  cwd       DIR        9,3       4096          2 /
init          1      root  rtd       DIR        9,3       4096          2 /
init          1      root  txt       REG        9,3      38620     146434 /sbin/init
init          1      root  mem       REG        9,3     125736     175507 /lib/ld-2.5.so
init          1      root  mem       REG        9,3    1602164     175514
/lib/i686/nosegneg/libc-2.5.so
init          1      root  mem       REG        9,3      16428     175518 /lib/libdl-2.5.so
init          1      root  mem       REG        9,3      93508     175677 /lib/libselinux.so.1
init          1      root  mem       REG        9,3     242880     175573 /lib/libsepol.so.1
init          1      root   10u     FIFO       0,15                  1543 /dev/initctl
```

Para visualizar más cómodamente esta salida, se puede utilizar el mandato **less** o el mandato **more** como subrutinas. Ejemplo:

```
lsof | less
```

Puede especificarse que se muestren todos los procesos desde un directorio en particular, solamente especificando este luego de **lsof**. En el siguiente ejemplo se solicita a **lsof** mostrar todos los procesos que estén haciendo uso de algo dentro de /var.

```
lsof /var
```

La salida de la anterior puede ser similar a la siguiente:

```
COMMAND     PID   USER   FD   TYPE DEVICE       SIZE     NODE NAME
auditd     2247   root    5w   REG    9,1     408058  5341208 /var/log/audit/audit.log
syslogd    2281   root    1w   REG    9,1    1134708 17006593 /var/log/messages
syslogd    2281   root    2w   REG    9,1      12461 17006594 /var/log/secure
syslogd    2281   root    3w   REG    9,1       9925 17006595 /var/log/maillog
syslogd    2281   root    4w   REG    9,1       3339 17006598 /var/log/cron
syslogd    2281   root    5w   REG    9,1          0 17006596 /var/log/spooler
syslogd    2281   root    6w   REG    9,1        916 17006597 /var/log/boot.log
named      2350  named  cwd    DIR    9,1       4096 16351240 /var/named/chroot/var/named
named      2350  named  rtd    DIR    9,1       4096 16351236 /var/named/chroot
named      2350  named    9r   CHR    1,8            16351246 /var/named/chroot/dev/random
rpc.statd  2407   root  cwd    DIR    9,1       4096 15433729 /var/lib/nfs/statd
rpc.statd  2407   root    8w   REG    9,1          5 25591831 /var/run/rpc.statd.pid
```

Si se quiere mostrar solamente el archivo utilizado por un procesos en particular, se utiliza la opción -p seguida del número de proceso. En el siguiente ejemplo se solicita a **lsof** mostrar los archivos utilizados por el proceso 2281 que arbitrariamente se ejecuta en un sistema:

```
lsof -p 2281
```

Si hubiera un proceso 2281, la salida podría verse como la siguiente:

```
COMMAND  PID USER   FD   TYPE     DEVICE    SIZE     NODE NAME
syslogd 2281 root  cwd    DIR        9,3    4096        2 /
syslogd 2281 root  rtd    DIR        9,3    4096        2 /
syslogd 2281 root  txt    REG        9,3   35800   146392 /sbin/syslogd
syslogd 2281 root  mem    REG        9,3 1602164   175514 /lib/i686/nosegneg/libc-2.5.so
syslogd 2281 root  mem    REG        9,3   46680   175529 /lib/libnss_files-2.5.so
syslogd 2281 root  mem    REG        9,3  125736   175507 /lib/ld-2.5.so
syslogd 2281 root    0u  unix 0xc0acfc80            6909 /dev/log
syslogd 2281 root    1w   REG        9,1 1134708 17006593 /var/log/messages
syslogd 2281 root    2w   REG        9,1   12461 17006594 /var/log/secure
syslogd 2281 root    3w   REG        9,1    9925 17006595 /var/log/maillog
syslogd 2281 root    4w   REG        9,1    3339 17006598 /var/log/cron
syslogd 2281 root    5w   REG        9,1       0 17006596 /var/log/spooler
syslogd 2281 root    6w   REG        9,1     916 17006597 /var/log/boot.log
```

La opción **-i** hará que se muestren todos los archivos de red (**Internet** y **x.25**) utilizados por procesos de red. Si se quiere mostrar los archivos de red en uso por algún proceso de red en particular, se utilizan las opciones **-i** seguido de una subrutina con **grep** y el nombre de algún servicio. En el siguiente ejemplo se pide a **lsof** mostrar solamente los archivos de red utilizados por los procesos de red derivados de **named**:

```
lsof -i | grep named
```

Lo anterior puede devolver una salida similar a la siguiente.

```
named      2350  named   20u  IPv4    7091       UDP localhost.localdomain:domain
named      2350  named   21u  IPv4    7092       TCP localhost.localdomain:domain (LISTEN)
named      2350  named   22u  IPv4    7093       UDP servidor.redlocal.net:domain
named      2350  named   23u  IPv4    7094       TCP servidor.redlocal.net:domain (LISTEN)
named      2350  named   24u  IPv4    7095       UDP *:filenet-tms
named      2350  named   25u  IPv6    7096       UDP *:filenet-rpc
named      2350  named   26u  IPv4    7097       TCP localhost.localdomain:rndc (LISTEN)
named      2350  named   27u  IPv6    7098       TCP localhost6.localdomain6:rndc (LISTEN)
named      2350  named   28u  IPv4 1153790       UDP 192.168.122.1:domain
```

21. Funciones básicas de vi

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

21.1. Introducción.

Vi es uno de los editores de texto más poderos y añejos que hay en el mundo de la informática. Resulta sumamente útil conocer la funcionalidad básica de Vi con la finalidad de facilitar la edición de archivos de texto simple, principalmente archivos de configuración.

21.2. Procedimientos.

21.2.1. Equipamiento lógico necesario.

Por lo general, vi se instala de modo predefinido en la mayoría de las distribuciones de GNU/Linux a través del paquete **vim-minimal** (CentOS, Fedora™ y Red Hat™ Enterprise Linux) o vim-base (openSUSE™ y SUSE™ Linux Enterprise). Puede conseguirse funcionalidad adicional a través de los siguientes paquetes:

- **vim-enhanced** Versión mejorada de vi que añade color a la sintaxis y otras mejoras en la interfaz. Instala **/usr/bin/vim** en CentOS, Fedora™, Red Hat™ Enterprise Linux y openSUSE™. Este paquete está ausente en SUSE™ Linux Enterprise.
- **vim-minimal**o **vim-base**: Versión muy básica y ligera de vi. Instala **/bin/vi**.
- **vim-X11** o **gvim**: Versión de vi para modo gráfico, más fácil de utilizar gracias a los menús y barra de herramientas. Instala **/usr/bin/gvim** y los enlaces simbólicos **/usr/bin/evim** y **/usr/bin/vimx** que apuntan hacia éste.

En CentOS, Fedora™ y Red Hat™ Enterprise Linux.

Si realizó una instalación mínima, instale vim ejecutando lo siguiente:

```
yum -y install vim vim-enhanced vim-minimal
```

21.2.1.1. En openSUSE™ y SUSE™ Linux Enterprise.

Si realizó una instalación mínima, instale vim ejecutando lo siguiente:

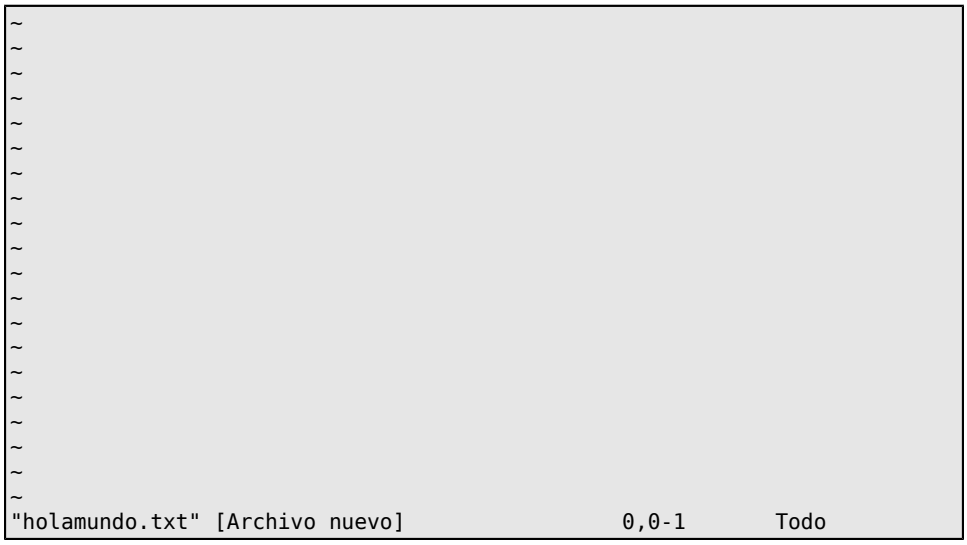
```
yast -i vim vim-base
```

21.3. Conociendo vi.

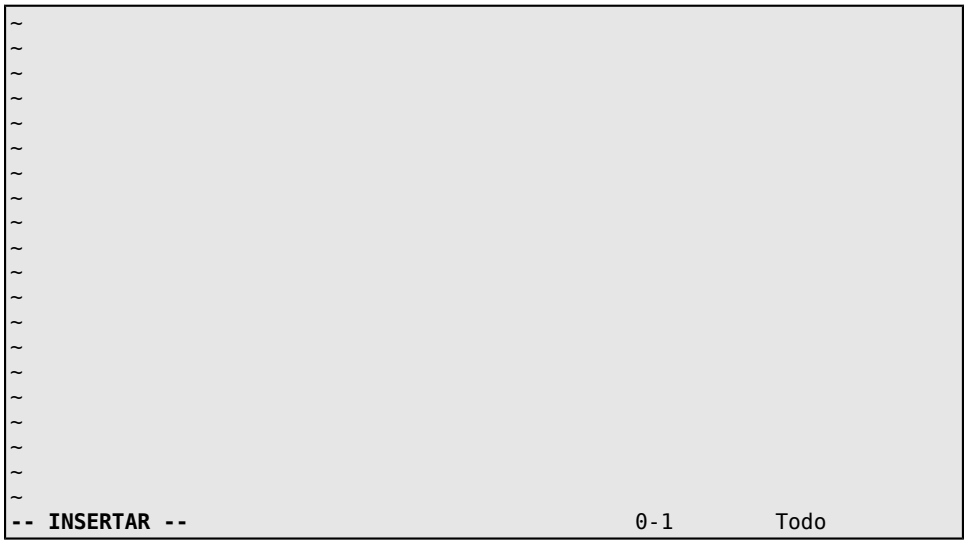
Acceda al sistema autenticando como usuario sin privilegios **(fulano)** y realice lo siguiente:

```
vim holamundo.txt
```

Lo anterior mostrará una interfaz como la siguiente:



Pulse una vez el botón <INSERT> —o bien la tecla i— y observe los cambios en la pantalla



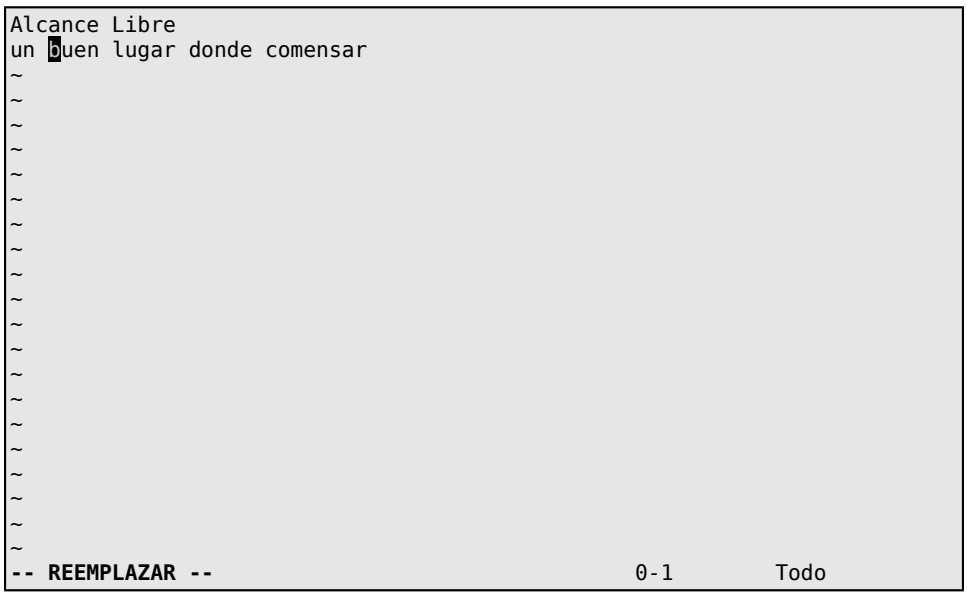
En la parte inferior de la pantalla aparecerá la palabra «**INSERTAR**». Esto significa que, al igual que cualquier otro editor de texto conocido, puede comenzar a insertar texto en el archivo. Escriba la frase «Alcance Libre», pulse la tecla ⏎ (**ENTER**) y **escriba de forma pro-positiva** la frase «un vuen lugar donde comensar»:

```
Alcance Libre
un vuen lugar donde comensar
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
-- INSERTAR --                                    0-1        Todo
```

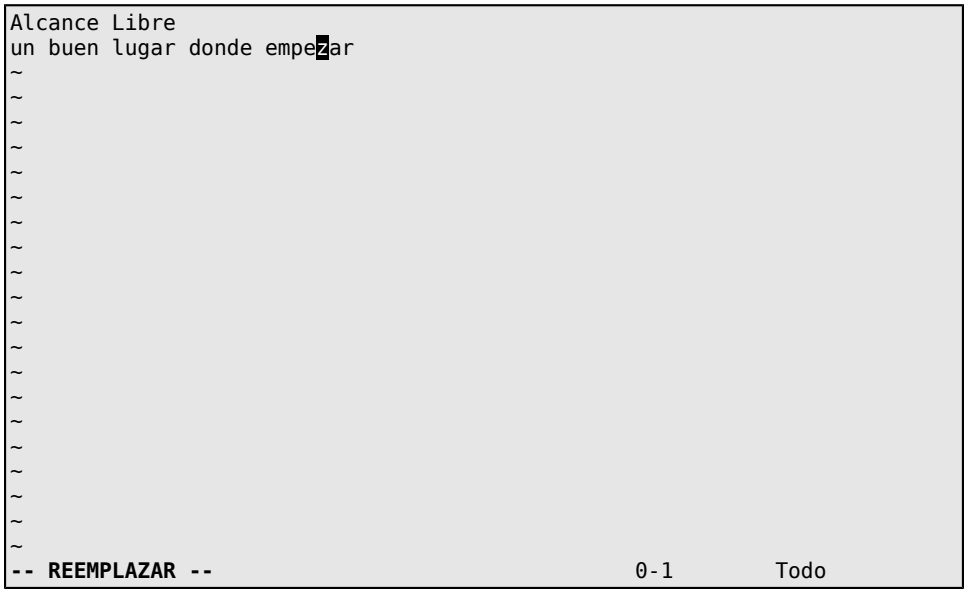
Posicione el cursor del teclado justo debajo de la «v» de la palabra «vuen» y pulse de nuevo la tecla <INSERT> del teclado —o bien pulse la tecla <Esc> y SHIFT+R. Notará que ahora aparece la palabra «REEMPLAZAR»:

```
Alcance Libre
un vuen lugar donde comensar
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
-- REEMPLAZAR --                                  0-1        Todo
```

Pulse la tecla «b» y observe como se reemplaza la letra «v» para quedar la palabra corregida como «buen»:



Mueva el cursor con las flechas del teclado y repita el procedimiento reemplazando la letra «s» por una «z» en la palabra «comensar» de modo que quede como «comenzar»:



Pulse la tecla <Esc> para salir del modo de reemplazo e inmediatamente pulse la tecla : (dos puntos) seguido de la letra «w» con la finalidad de proceder a guardar el archivo en el sistema de archivos:

```
Alcance Libre
un buen lugar donde comenzar
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
:w
```

Pulse la tecla ⏎ (**ENTER**) y notará que aparece un mensaje en la parte inferior de la pantalla que indicará que el archivo ha sido guardado:

```
Alcance Libre
un buen lugar donde comenzar
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"holamundo.txt" [Nuevo] 2L, 44C escritos        2,3         Todo
```

Vuelva a pulsar la tecla **:** (dos puntos) e luego escriba «saveas adiosmundo.txt»:

```
Alcance Libre
un buen lugar donde comenzar
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
:saveas adiosmunto.txt
```

Pulse nuevamente la tecla ⏎ (**ENTER**) y observe el mensaje en la parte inferior de la pantalla que indica el archivo acaba de ser guardado como el archivo adiosmundo.txt:

```
Alcance Libre
un buen lugar donde comenzar
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"adiosmundo.txt" [Nuevo] 2L, 44C escritos       2,3         Todo
```

Vuelva a pulsar la tecla «INSERT» para regresar al modo de inserción y escriba lo siguiente:

```
Alcance Libre
un buen lugar donde comenzar
Creo que el mundo es un lugar muy malo
La gente que conozco es mala
Mi vida ha sido muy mala
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
-- INSERTAR --                                5,24          Todo
```

A continuación pulse la tecla <Esc> e inmediatamente pulse la tecla **:** (dos puntos) seguido de la combinación de teclas **%s/mal/buen/g** del siguiente modo:

```
Alcance Libre
un buen lugar donde comenzar
Creo que el mundo es un lugar muy malo
La gente que conozco es mala
Mi vida ha sido muy mala
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
:%s/mal/buen/g
```

Pulse de nuevo la tecla ⏎ (**ENTER**) y observe como ha sido reemplazada la cadena de caracteres «mal» por la cadena de caracteres «buen» en todo el archivo, quedando del siguiente modo:

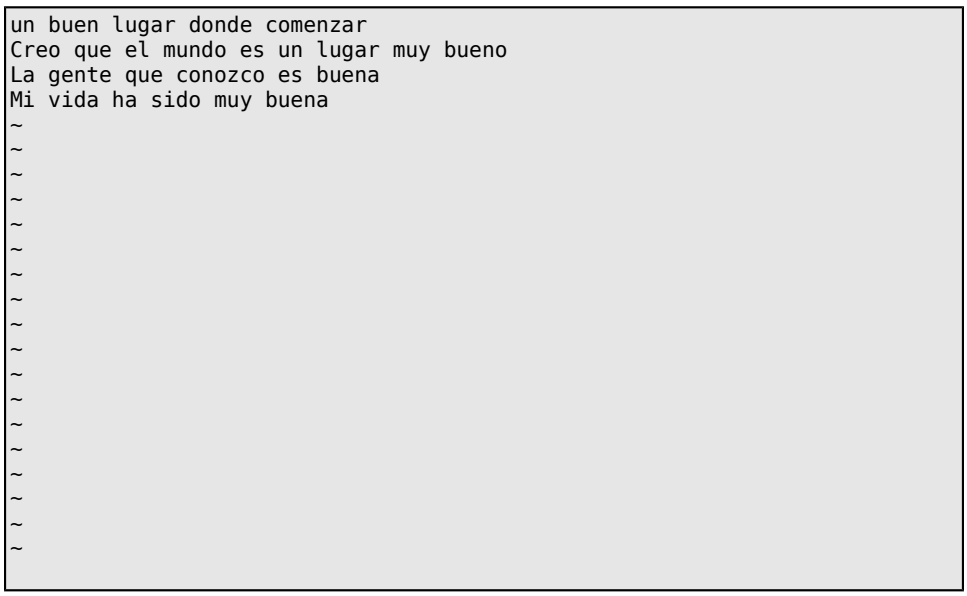
```
Alcance Libre
un buen lugar donde comenzar
Creo que el mundo es un lugar muy bueno
La gente que conozco es buena
Mi vida ha sido muy buena
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
3 sustituciones en 3 líneas                    5,1          Todo
```

En el procedimiento anterior, el símbolo «%» indicaba que se aplicaría un procedimiento a todo el archivo, además de la línea misma, la letra «s» indicaba que se realizaría la búsqueda de la cadena de caracteres «mal» definida después de la diagonal (/) por la cadena de caracteres «buen» en toda la línea, indicado por la letra «g».

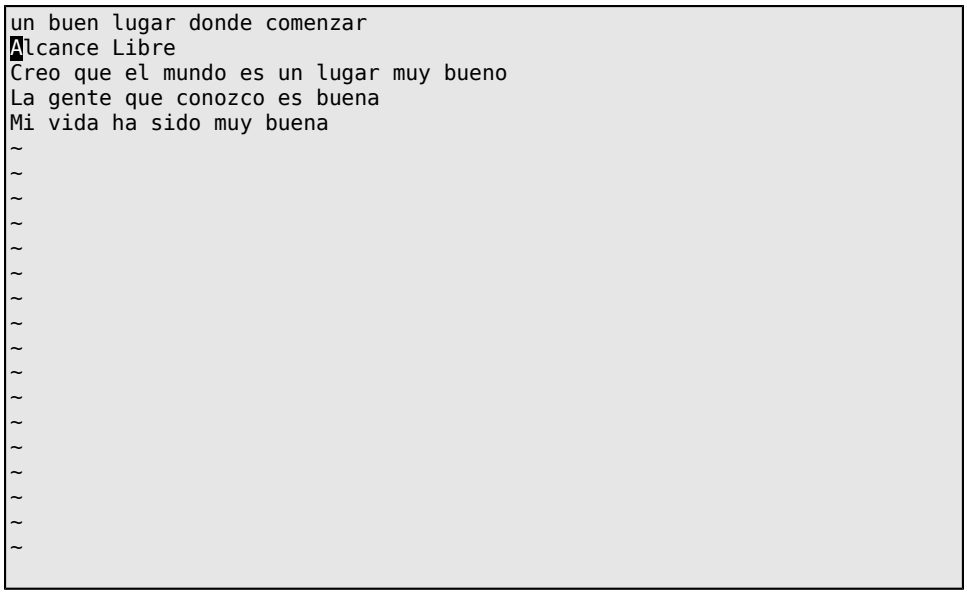
A continuación, posiciones el cursor de teclado utilizando las flechas del teclado hasta el primer carácter de la primera línea:

```
Acance Libre
un buen lugar donde comenzar
Creo que el mundo es un lugar muy bueno
La gente que conozco es buena
Mi vida ha sido muy buena
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
3 sustituciones en 3 líneas                    5,1          Todo
```

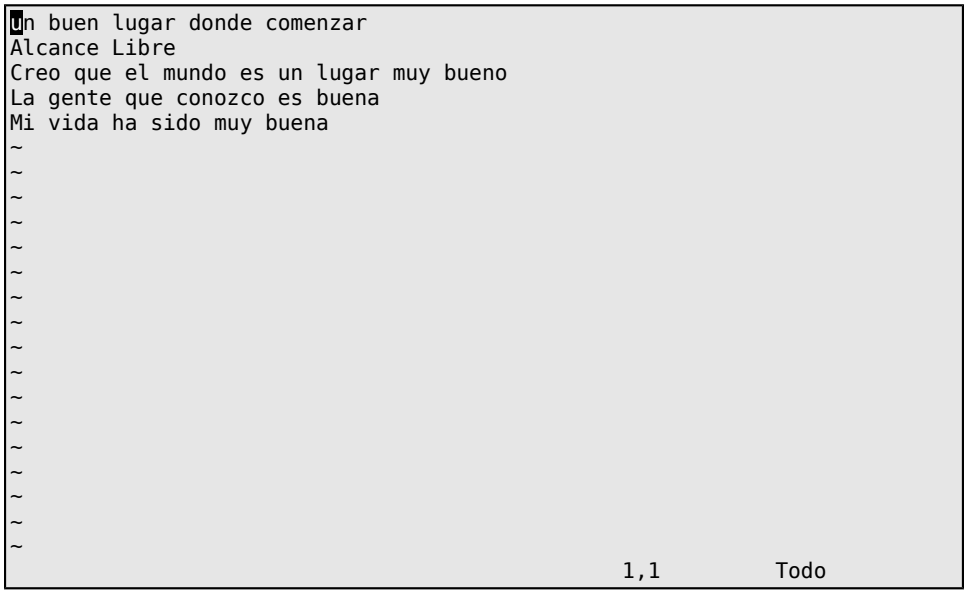
Ahora pulse dos veces consecutivas la tecla «d», es decir, pulsará «dd». Observe como desaparece la primera línea:



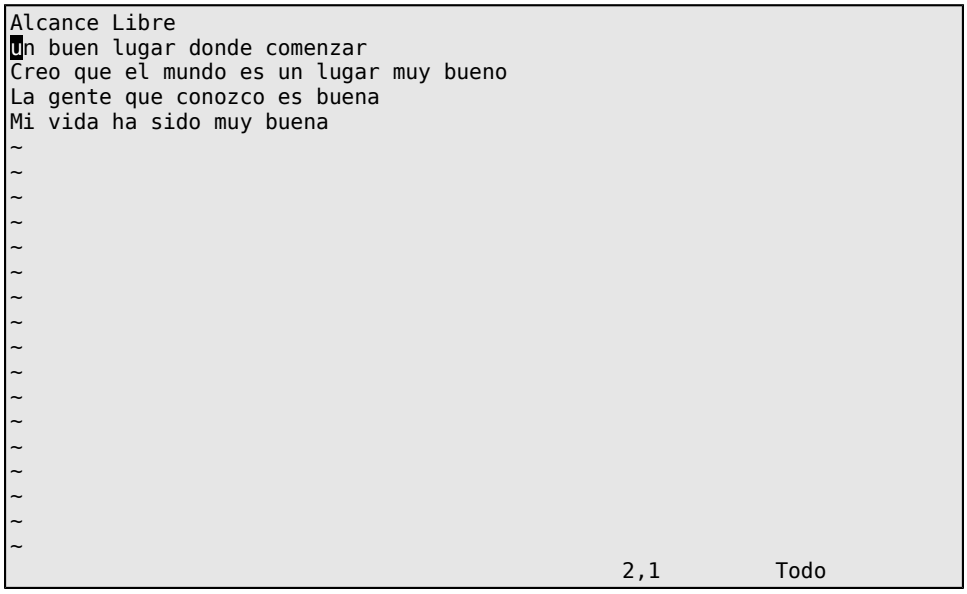
Pulse ahora la tecla «p» para volver a pegar la línea:



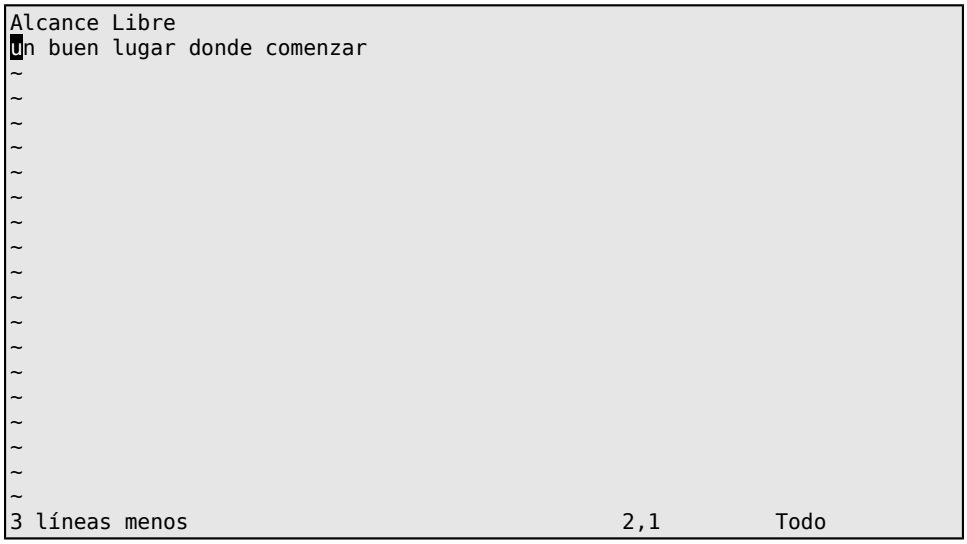
Observe que la línea «Alcance Libre» reapareció debajo de la línea «un buen lugar donde comenzar». Utilizando las flechas del teclado, coloque el cursor del teclado nuevamente sobre el primer carácter de la primera línea del archivo, es decir, sobre la letra «u» de la línea «un buen lugar donde comenzar»:



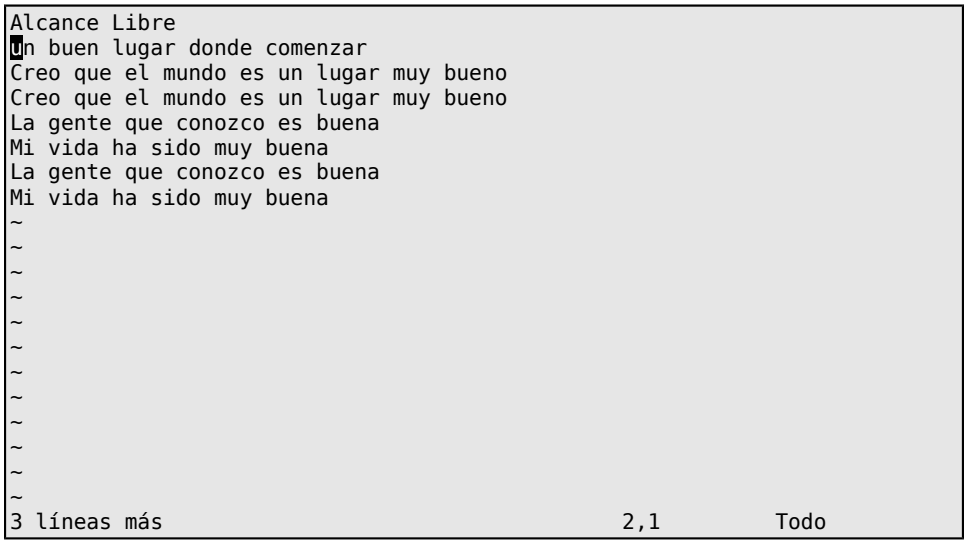
Vuelva a pulsar «dd» para cortar la línea «un buen lugar donde comenzar» e luego pulse la tecla «p» para pegar la línea en el lugar correcto:



Coloque ahora el cursor sobre la letra «C» de la línea «Creo que el mundo es un lugar muy bueno» y pulse la tecla «3» seguido de «dd» y observe como son cortadas las tres siguientes lineas:



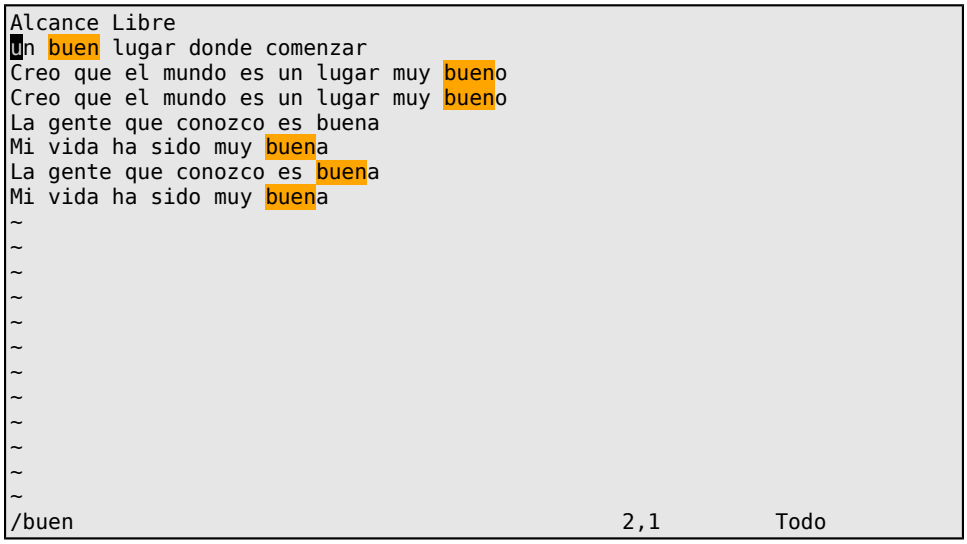
Pulse la tecla «p» una vez, observe el resultado. Vuelva a pulsar la tecla «p» y observe el resultado. Las dos acciones anteriores añadieron ahora 6 líneas restaurando las eliminadas anteriormente y agregando tres líneas más con el mismo contenido:



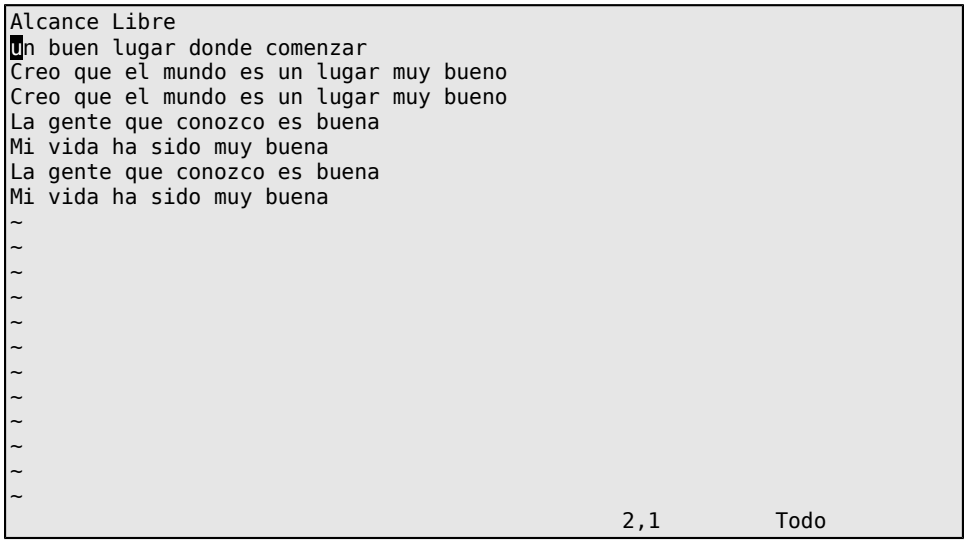
Pulse ahora la tecla **:** (dos puntos) seguido de la tecla «x» y la tecla ⏎ (**ENTER**) con la finalidad de salir del editor guardando el archivo.

SUSE™ Linux Enterprise carece del paquete **vim-enhanced**, por lo cual será imposible se muestre el resaltado de las búsquedas. Si utiliza este sistema operativo, omita los siguientes dos pasos.

Abra nuevamente el archivo **adiosmundo.txt** con vi y pulse la combinación de teclas **:/buen**, de modo que se realice una búsqueda de la cadena de caracteres «buen» y además se resalten las coincidencias:



Para cancelar el resaltado de los resultados, pulse la combinación de teclas **:nohl**:



Pulse **A** (combinación de las teclas SHIFT+a) mientras el cursor permanece en la segunda línea y observe que iniciará el modo **INSERTAR** colocando el cursor al final de la línea donde se encontraba:

```
Alcance Libre
un buen lugar donde comenzar
Creo que el mundo es un lugar muy bueno
Creo que el mundo es un lugar muy bueno
La gente que conozco es buena
Mi vida ha sido muy buena
La gente que conozco es buena
Mi vida ha sido muy buena
~
~
~
~
~
~
~
~
~
~
~
~
-- INSERTAR --                                  2,1         Todo
```

Pulse la tecla <Esc> y enseguida **o**. Notará que iniciará el modo **INSERTAR** abriendo una nueva línea:

```
Alcance Libre
un buen lugar donde comenzar

Creo que el mundo es un lugar muy bueno
Creo que el mundo es un lugar muy bueno
La gente que conozco es buena
Mi vida ha sido muy buena
La gente que conozco es buena
Mi vida ha sido muy buena
~
~
~
~
~
~
~
~
~
~
~
-- INSERTAR --                                  3,1         Todo
```

Pulse nuevamente la tecla <Esc> y en seguida la combinación **dG** (d, luego SHIFT+G). Notará que elimina todo el contenido del texto desde la posición del cursor hasta el final del archivo:

```
Alcance Libre
Un buen lugar donde comenzar
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
7 líneas menos                                  2,1         Todo
```

Pulse la combinación **:u** y notará que el cambio se ha descartado, regresando las 7 líneas que habían sido eliminadas:

```
Alcance Libre
un buen lugar donde comenzar

Creo que el mundo es un lugar muy bueno
Creo que el mundo es un lugar muy bueno
La gente que conozco es buena
Mi vida ha sido muy buena
La gente que conozco es buena
Mi vida ha sido muy buena
~
~
~
~
~
~
~
~
~
~
~
~
7 líneas más                                    3,0-1       Todo
```

21.4. Otros mandatos de vi.

Mandato	Resultado
i [o bien la tecla insert]	Inicia el modo insertar **antes** del cursor
R (r + SHIFT)	Inicia el modo reemplazar al **inicio** de la línea donde se encuentra el cursor
a	Inicia insertar texto **después** del cursor
I (i + SHIFT)	Inicia insertar texto al **inicio** de la línea donde se encuentra el cursor
A (a + SHIFT)	Inicia insertar texto al **final** de la línea donde se encuentra el cursor.
o	Abre una nueva línea e inicia insertar texto en la nueva línea.
x	Elimina el carácter que esté sobre el cursor.
dd	Elimina o corta la línea actual donde se encuentre el cursor.
yy	Copia la línea actual donde se encuentre el cursor.

D	Elimina desde la posición actual del cursos hasta el final de la misma línea donde se encuentra el cursor.
dG	Elimina todo hasta el final del archivo.
:q	Salida. Si hay cambios pendientes se impedirá la salida.
:q!	Salida descartando los cambios en el archivo.
:w	Guardar el archivo sin salir.
:wq	Guardar el archivo y sale de vi.
:x	lo mismo que :wq
:saveas /lo/que/sea	guarda el archivo como otro archivo donde sea necesario.
:wq! ++enc=utf8	codifica el archivo en UTF-8.
:u	deshacer cambios
:red	rehacer cambios.
:/cadena de caracteres	Búsqueda de cadenas de caracteres.
:nohl	Cancelar el resaltado de resultados de Búsqueda.
:e archivo	Edita un nuevo archivo en un nuevo búfer.
:bn o :bnext	Conmuta al siguiente archivo abierto.
:bp o :bprev	Conmuta al archivo abierto anterior.
:bd	Cierra búfer activo.
CTRL+W s o :split	Divide horizontalmente en dos búferes.
CTRL+W v	Divide verticalmente en dos búferes.
CTRL+W w	Conmuta entre en búferes abiertos.
CTRL+W s	Cierra el búfer activo.

21.5. Más allá de las funciones básicas.

Instale el paquete vim-enhanced:

```
yum -y install vim-enhanced
```

Utilice **vimtutor** y complete el **tutor interactivo oficial** de Vi con la finalidad de que conozca el resto de las funcionalidades más importantes.

22. Introducción a sed

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales (incluyendo su publicación, a través de cualquier medio, por entidades con fines de lucro). c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en castellano. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

22.1. Introducción.

22.1.1. Acerca de sed.

Sed es un editor de emisiones (**s**tream **ed**itor) utilizado para el procesamiento de texto en archivos. Utiliza un lenguaje de programación para realizar transformaciones en una emisión de datos leyendo línea por línea de estos. Fue desarrollado entre 1973 y 1974 por Lee E. McMahon de Bell Labs. Está incluido en las instalaciones básicas de prácticamente todas las distribuciones de GNU/Linux.

22.2. Procedimientos.

A continuación se mostrarán ejemplos del uso de **sed**.

Utilice vi para crear el archivo usuario.txt:

```
vi usuario.txt
```

Ingrese el siguiente contenido y salga de vi:

```
Fulano Algo
Calle Mengana 123
Colonia Perengana
Ciudad de Zutano, C.P. 123456
```

Si utiliza el mandato cat sobre el archivo, visualizará tal cual el contenido de usuario.txt como fue ingresado en vi.

```
cat usuario.txt
```

Si se quiere convertir a doble espacio la salida del archivo usuario.txt, utilice el siguiente mandato:

```
sed G usuario.txt
```

La salida devolverá lo siguiente:

```
Fulano Algo

Calle Mengana 123

Colonia Perengana

Ciudad de Zutano, C.P. 123456
```

Para guardar esta salida en el archivo usuario2.txt, utilice lo siguiente:

```
sed G usuario.txt > usuario2.txt
```

Si se quiere convertir a doble espacio la salida del archivo usuario.txt, utilice el siguiente mandato:

```
sed 'G;G' usuario.txt
```

La salida devolverá lo siguiente:

```
Fulano Algo
Calle Mengana 123
Colonia Perengana
Ciudad de Zutano, C.P. 123456
```

Para guardar esta salida en el archivo usuario2.txt, utilice lo siguiente:

```
sed 'G;G' usuario.txt > usuario3.txt
```

El contenido de usuario3.txt tendrá triple espacio de separación. Si se desea convertir un archivo a doble espacio, pero que no haya más de una línea vacía entre cada lñíena con datos, se utiliza lo siguiente:

```
sed '/^$/d;G' usuario3.txt
```

La salida devolverá lo siguiente:

```
Fulano Algo
Calle Mengana 123
Colonia Perengana
Ciudad de Zutano, C.P. 123456
```

Si se desea eliminar el doble espacio del archivo usuario2.txt, se utiliza lo siguiente:

```
sed 'n;d' usuario2.txt
```

La salida devolverá lo siguiente:

```
Fulano Algo
Calle Mengana 123
Colonia Perengana
Ciudad de Zutano, C.P. 123456
```

Si se quiere agregar una línea en blanco arriba de toda línea que contenga la expresión regular **enga**, se utiliza lo siguiente:

```
 sed '/enga/{x;p;x;}' usuario.txt
```

La salida devolverá lo siguiente:

```
Fulano Algo
Calle M**enga**na 123
Colonia P**eren**gana
```

```
Ciudad de Zutano, C.P. 123456
```

Si se quiere agregar una línea en blanco debajo de toda línea que contenga la expresión regular **3**, se utiliza lo siguiente:

```
sed '/3/G' usuario.txt
```

La salida devolverá lo siguiente:

```
Fulano Algo
Calle Mengana 123
Colonia Perengana
Ciudad de Zutano, C.P. 123456
```

Si se quiere agregar una línea en blanco arriba y debajo de toda línea que contenga la expresión regular **3**, se utiliza lo siguiente:

```
sed '/3/{x;p;x;G;}' usuario.txt
```

La salida devolverá lo siguiente:

```
Fulano Algo
Calle Mengana 123
Colonia Perengana
Ciudad de Zutano, C.P. 123456
```

Para reemplazar texto se utiliza el modelo 's/texto/nuevo-texto/' donde texto puede ser también una expresión regular. En el siguiente ejemplo se reemplazarán las incidencias del número por el número 9:

```
sed 's/3/9/g' usuario.txt
```

La salida devolverá lo siguiente:

```
Fulano Algo
Calle Mengana 129
Colonia Perengana
Ciudad de Zutano, C.P. 129456
```

En el siguiente ejemplo se reemplazan los espacios por tabuladores a todo lo largo de todas las líneas:

```
sed 's/\ /\t/g' usuario.txt
```

La salida devolverá lo siguiente:

```
Fulano  Algo
Calle   Mengana 123
Colonia Perengana
Ciudad  de Zutano,      C.P.    123456
```

En el siguiente ejemplo se reemplazan solo el primer espacio de cada línea por un tabulador:

```
sed 's/\ /\t/' usuario.txt
```

La salida devolverá lo siguiente:

```
Fulano  Algo
Calle   Mengana 123
Colonia Perengana
Ciudad  de Zutano, C.P. 123456
```

La siguiente línea añade 5 espacios al inicio de cada línea:

```
sed 's/^/     /' usuario.txt
```

La salida devolverá lo siguiente:

```
     Fulano Algo
     Calle Mengana 123
     Colonia Perengana
     Ciudad de Zutano, C.P. 123456
```

El siguiente mandato solo imprime la primera línea del archivo usuario.txt:

```
sed q usuario.txt
```

La salida devolverá lo siguiente:

```
Fulano Algo
```

El siguiente mandato solo imprime las primeras dos líneas del archivo usuario.txt:

```
sed 2q usuario.txt
```

La salida devolverá lo siguiente:

```
Fulano Algo
Calle Mengana 123
```

El siguiente mandato solo muestra las últimas tres líneas del archivo usuario.txt:

```
sed -e :a -e '$q;N;4,$D;ba' usuario.txt
```

La salida devolverá lo siguiente:

```
Calle Mengana 123
Colonia Perengana
Ciudad de Zutano, C.P. 123456
```

El siguiente mandato solo mostrará las líneas que incluyen **3**:

```
sed '/3/!d' usuario.txt
```

La salida devolverá lo siguiente:

```
Calle Mengana 123
Ciudad de Zutano, C.P. 123456
```

El siguiente mandato solo mostrará las líneas que **no** incluyen **3**:

```
sed '/3/d' usuario.txt
```

La salida devolverá lo siguiente:

```
Fulano Algo
Colonia Perengana
```

El siguiente mandato pide mostrar la linea que está inmediatamente después de la expresión **Fulano**, pero no la línea en si que incluye **Fulano**:

```
sed -n '/Fulano/{n;p;}' usuario.txt
```

La salida devolverá lo siguiente:

```
Calle Mengana 123
```

El siguiente mandato pide mostrar la linea que está inmediatamente antes de la expresión **Calle**, pero no la línea en si que incluye **Calle**:

```
sed -n '/Calle/{g;1!p;};h' usuario.txt
```

La salida devolverá lo siguiente:

```
Fulano Algo
```

22.3. Bibliografía.

- Eric Pement: http://student.northpark.edu/pemente/sed/sed1line.txt
- Wikipedia: http://en.wikipedia.org/wiki/Sed

23. Introducción a AWK

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales (incluyendo su publicación, a través de cualquier medio, por entidades con fines de lucro). c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en castellano. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

23.1. Introducción.

23.1.1. Acerca de AWK.

AWK, cuyo nombre deriva de la primera letra de los apellidos de sus autores Alfred **A**ho, Peter **W**einberger y Brian **K**ernighan, es un lenguaje de programación que fue diseñado con el objetivo de procesar datos basados sobre texto y una de las primeras herramientas en aparecer en Unix. Utiliza listas en un índice ordenado por cadenas clave (listas asociativas) y expresiones regulares. Es un lenguaje ampliamente utilizado para la programación de guiones ejecutables pues añade funcionalidad a las tuberías en los sistemas operativos tipo **POSIX**. Está incluido en las instalaciones básicas de prácticamente todas las distribuciones de GNU/Linux.

23.1.2. Estructura de los programas escritos en AWK.

El mandato **awk** utiliza un archivo o emisión de ordenes y un archivo o emisión de entrada. El primero indica como procesar al segundo. El archivo de entrada es por lo general texto con algún formato que puede ser un archivo o bien la salida de otro mandato.

La sintaxis general utilizada para el mandato **awk** utiliza el siguiente patrón:

```
awk 'expresión-regular { orden }'
```

Cuando se utiliza el mandato **awk**, éste examina el archivo de entrada y ejecuta la orden cuando encuentra la expresión regular especificada.

El siguiente modelo ejecutaría la orden al inicio del programa y antes de que sean procesados los datos del archivo de entrada:

```
awk 'BEGIN { orden }'
```

El siguiente modelo ejecutaría la orden al final del programa y después de que sean procesados los datos del archivo de entrada:

```
awk 'END { orden }'
```

El siguiente modelo ejecutaría la orden por cada una de las líneas del archivo de entrada:

```
awk '{ orden }'
```

23.2. Procedimientos.

A continuación se mostrarán ejemplos del uso de AWK.

El siguiente mandato específica que al inicio se imprima en la salida la frase "Hola mundo" y terminar el procesamiento.

```
awk 'BEGIN { print "Hola mundo"; exit }'
```

Lo anterior deberá devolver una salida como la siguiente:

```
Hola mundo
```

Si se genera el archivo **prueba.txt** del siguiente modo:

```
echo -e "Columna1\tColumna2\tColumna3\tColumna4\n" > ejemplo.txt
```

Y se visualiza con el mandato cat:

```
cat ejemplo.txt
```

Devolverá el siguiente contenido:

```
Columna1        Columna2        Columna3        Columna4
```

Si se utiliza el mandato **awk** para que solo muestre la columna 1 y la columna 3 del siguiente modo:

```
awk '{ print $1, $3}' ejemplo.txt
```

La salida devolverá lo siguiente:

```
Columna1 Columna3
```

Si se utiliza el mandato **awk** para que solo muestre la columna 3 y la columna 1, en ese orden, del siguiente modo:

```
awk '{ print $3, $1}' ejemplo.txt
```

La salida devolverá lo siguiente:

```
Columna3 Columna1
```

Si se añaden datos al archivo **ejemplo.txt** del siguiente modo:

```
echo -e "Dato1\tDato2\tDato3\tDato4\n" >> ejemplo.txt
echo -e "Dato5\tDato6\tDato7\tDato8\n" >> ejemplo.txt
echo -e "Dato9\tDato10\tDato11\tDato12\n" >> ejemplo.txt
```

Y se visualiza con el mandato cat:

```
cat ejemplo.txt
```

Devolverá el siguiente contenido:

```
Columna1        Columna2        Columna3        Columna4
Dato1   Dato2   Dato3   Dato4
Dato5   Dato6   Dato7   Dato8
Dato9   Dato10  Dato11  Dato12
```

Si se utiliza nuevamente el mandato **awk** para que solo muestre la columna 1 y la columna 3 del siguiente modo:

```
awk '{ print $1, $3 }' ejemplo.txt
```

La salida devolverá lo siguiente:

```
Columna1 Columna3
Dato1 Dato3
Dato5 Dato7
Dato9 Dato11
```

Si se utiliza el mandato **awk** del siguiente modo para que solo muestre solo la línea cuya columna contenga la expresión regular Dato5:

```
awk '/Dato5/ { print }' ejemplo.txt
```

La salida devolverá lo siguiente:

```
Dato5   Dato6   Dato7   Dato8
```

Si se utiliza el mandato **awk** del siguiente modo para que solo muestre solo la línea cuya columna contenga la expresión regular Dato5 y además solo las columnas 1 y 4:

```
awk '/Dato5/ { print $1, $4}' ejemplo.txt
```

La salida devolverá lo siguiente:

```
Dato5 Dato8
```

Si se utiliza el mandato **awk** del siguiente modo para que muestre solo las líneas con **más de 35 caracteres** en el archivo **/etc/crontab**:

```
awk 'length > 35' /etc/crontab
```

La salida devolverá algo similar a lo siguiente:

```
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# *  *  *  *  * user-name  command to be executed
```

Si se utiliza el mandato **awk** del siguiente modo para que muestre solo las líneas con **menos de 35 caracteres** en el archivo **/etc/crontab**:

```
awk 'length < 35' /etc/crontab
```

La salida devolverá algo similar a lo siguiente:

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root

# For details see man 4 crontabs

# Example of job definition:
# |  .------------- hour (0 - 23)
# |  |  |  |  |
```

Utilice el mandato **vi** para crear el archivo **usuario.txt**:

```
vi usuario.txt
```

Añada el siguiente contenido:

```
Fulano Algo
Calle Mengana 123
Colonia Perengana
Ciudad de Zutano, C.P. 123456
```

Para que el mandato **awk** reconozca cada línea como un registro completo, en lugar de considerar cada palabra como una columna, se utiliza **'BEGIN { FS="\n" ; RS="" }'**, donde el valor de **FS** (**F**ield **S**eparator o separador de campo) se establece como un retorno de carro y el valor de **RS** (**R**ecord **S**eparator o separador de registro) se establece como una línea vacía. Si utiliza el siguiente mandato donde se establecen los valores mencionados para FS y RS y se pide se impriman los valores de cada registro (cada línea) separados por una coma y un espacio:

```
awk 'BEGIN { FS="\n"; RS="" } \
    { print $1 ", " $2 ", " $3 ", " $4 }' usuario.txt
```

La salida devolverá lo siguiente:

```
Fulano Algo, Calle Mengana 123, Colonia Perengana, Ciudad de Zutano, C.P. 123456
```

El mandato **awk** puede realizar conteo de líneas, palabras y caracteres. El siguiente mandato se establece que el valor de **w** sea igual al número de campos (**N**ew **F**ield o **NF**), **c** sea igual la longitud de cada campo y que se imprima el número de campos, el valor de **w** y el valor de **c**:

```
awk '{ w += NF; c += length } \
    END { print \
    "Campos: " NR , "\nPalabras: " w, "\nCaracteres: " c }' \
    usuario.txt
```

La salida devolverá lo siguiente:

```
Campos: 4
Palabras: 12
Caracteres: 74
```

Genere el archivo **numeros.txt** con el siguiente contenido, donde las columnas serán separadas por un tabulador:

```
1 2 3 4
5 6 7 8
9 10 11 12
```

el mandato **awk** puede realizar operaciones matemáticas. El siguiente mandato establece que la variable ***s*** es igual a la suma del valor de los campos de la **primera columna** del archivo **numeros.txt** e imprime el valor de **s**:

```
awk '{ s += $1 } END { print s }' numeros.txt
```

La salida devolverá lo siguiente (que corresponde al resultado de la suma de 1+5+9):

```
15
```

Si se hace lo mismo, pero con los valores de la columna 2:

```
awk '{ s += $2 } END { print s }' numeros.txt
```

La salida devolverá lo siguiente (que corresponde al resultado de la suma de 2+6+10):

```
18
```

Para hacer conteo de frecuencia de palabras, Se establece que el valor para **FS** (**F**ield **S**eparator o separador de línea) sea igual a expresiones regulares que van desde la letra **a** hasta la letra **z** y desde la letra **A** hasta la letra **Z**, se establece que el valor de la variable ***i*** es igual a **1** y menor al número de campos.

```
awk 'BEGIN { FS="[^a-zA-Z]+" } \
    { for (i=1; i<=NF; i++) words[tolower($i)]++ } \
    END { for (i in words) print i, words[i] }' /etc/crontab
```

La salida devolverá algo similar a lo siguiente:

```
 15
job 1
to 1
usr 2
root 1
shell 1
mon 1
hour 1
bin 3
executed 1
name 1
wed 1
fri 1
details 1
of 3
feb 1
week 1
sun 1
path 1
crontabs 1
or 3
be 1
apr 1
definition 1
month 2
sbin 2
tue 1
jan 1
day 2
command 1
for 1
sunday 1
man 1
mar 1
user 1
minute 1
example 1
see 1
bash 1
sat 1
mailto 1
thu 1
```

24. Uso de los mandatos chown y chgrp

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

24.1. Introducción.

Tanto el mandato **chown** como el mandato **chgrp** forman parte del paquete **coreutils**, el cual se instala de forma predeterminada en todas las distribuciones de GNU/Linux debido a que se trata componente esencial.

URL: ftp://alpha.gnu.org/gnu/coreutils/

24.2. Mandato chown.

El mandato **chown** se utiliza para cambiar el propietario al cual pertenece un archivo o directorio. Puede especificarse tanto el nombre de un usuario, así como un número de identidad de usuario (**UID**). De manera opcional, utilizando un signo de dos puntos (**:**) o bien un punto (**.**), permite especificar también un nombre de grupo.

El manual completo del mandato **chown** puede consultarse ejecutando lo siguiente:

```
man 1 chown
```

24.2.1. Opciones.

-R	De manera descendente cambia el propietario de los directorios junto con todos sus contenidos. De manera opcional también permite cambiar el grupo al cual pertenecen.
-v (o --verbose)	Salida más descriptiva.
--version	Ver el número de versión del programa.
--dereference	Actúa sobre enlaces simbólicos en lugar de hacerlo sobre el destino.
-h (o --no-dereference)	En el caso de enlaces simbólicos, cambia el propietario del destino en lugar del propio enlace.
--reference	Cambia el el propietario de un archivo, tomando como referencia el propietario de otro.

24.2.2. Utilización.

```
chown [opciones] usuario[:grupo] archivo(s) o directorio(s)
```

24.3. Mandato chgrp.

El mandato **chgrp** se utiliza para cambiar el grupo al cual pertenece un archivo o directorio. Puede especificarse tanto el nombre de un grupo, así como un número de identidad de grupo (**GID**).

El manual completo del mandato **chgrp** puede consultarse ejecutando lo siguiente:

```
man 1 chgrp
```

24.3.1. Opciones.

-R	De manera descendente cambia el grupo al cual pertenecen los directorios junto con todos sus contenidos.
-v (o --verbose)	Salida de **chgrp** más descriptiva.
--version	Ver el número de versión del programa.
--dereference	Actúa sobre enlaces simbólicos en lugar de hacerlo sobre el destino.
-h (o --no-dereference)	En el caso de enlaces simbólicos cambia el grupo del destino en lugar del propio enlace.
--reference	Cambia el grupo de un archivo tomando como referencia el propietario de otro.

24.3.2. Utilización.

```
chgrp [opciones] archivo(s) o directorio(s)
```

24.4. Ejemplos.

El siguiente mandato realiza el cambio de propietario a **fulano** sobre el archivo algo.txt.

```
chown fulano algo.txt
```

El siguiente mandato realiza el cambio de propietario a **fulano** y el grupo **desarrollo** sobre el archivo algo.txt.

```
chown fulano:desarrollo algo.txt
```

El siguiente mandato realiza el cambio de propietario a **fulano** y el grupo **mail** del sub-directorio **Mail** junto con todo su contenido.

```
chown -R fulano:mail Mail
```

El siguiente mandato realiza el cambio de grupo a **desarrollo** sobre el archivo algo.txt.

```
chgrp desarrollo algo.txt
```

25. Permisos del Sistema de Archivos en GNU/Linux.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

25.1. Introducción.

En los sistemas operativos tipo **POSIX** cada elemento del sistema de archivos, como archivos, directorios, enlaces simbólicos, etc., tiene la característica de poseer permisos que lo ubican dentro del mismo. Éstos sirven como uno más de los niveles de seguridad del sistema operativo al impedir que cualquier usuario pueda leer, escribir, ejecutar o acceder a dichos archivos y directorios de manera arbitraria. Estos permisos vistos de manera básica son: **lectura** (**r**, *read*), **escritura** (**w**, *write*) y **ejecución** (**x**, *execution*) y se agrupan en bloques (**rwx**) para 3 diferentes clases (usuario, grupo y otros).

Los permisos de acceso de cada archivo y directorio del sistema son mostrados por un conjunto de 10 caracteres, los cuales proporcionan información acerca del tipo de elemento, junto con permisos para el usuario y grupo propietario para leer, escribir y ejecutar, como se muestra en el siguiente ejemplo:

```
-rwxr-xr-x 1 fulano fulano 0 jul 31 18:11 algo.txt
```

La asignación de permisos de acceso (de lectura, escritura y ejecución) pueden gestionarse a través de modos, los cuales consisten de combinaciones de números de tres dígitos (usuario, grupo y otros) y los mandatos **chmod** y **setfacl**.

25.2. Notación simbólica.

El esquema de notación simbólica se compone de 10 caracteres, donde el primer carácter indica el tipo de archivo:

Valor	Descripción
-	Archivo regular.
d	Directorio.
b	Archivo especial como dispositivo de bloque.
c	Archivo de carácter especial
l	Enlace simbólico.
p	Tubería nombrada (FIFO)
s	Zócalo de dominio (socket)

Como se mencionó anteriormente, cada clase de permisos es representada por un conjunto de tres caracteres. El primer conjunto de caracteres representa la clase del usuario, el segundo conjunto de tres caracteres representa la clase del grupo y el tercer conjunto representa la clase de «otros» (resto del mundo). Cada uno de los tres caracteres representa permisos de lectura, escritura y ejecución, respectivamente y en ese orden.

Ejemplos:

Permisos	Descripción
drwxr-xr-x	Directorio con permiso 755
crw-rw-r--	Archivo de carácter especial con permiso 664.
srwxrwxr-x	Zócalo con permiso 775.
prw-rw-r--	Tubería (FIFO) con permiso 664.
-rw-r--r--	Archivo regular con permiso 644.

25.3. Notación octal.

La notación octal consiste de valores de tres a cuatro dígitos en base-8. Con la notación octal de tres dígitos cada número representa un componente diferente de permisos a establecer: clase de usuario, clase de grupo y clase de otros (resto del mundo) respectivamente. Cada uno de estos dígitos es la suma de sus bits que lo componen (en el sistema numeral binario). Como resultado, bits específicos se añaden a la suma conforme son representados por un numeral:

- El Bit de ejecución (acceso en el caso de directorios) añade **1** a la suma.
- El bit de escritura añade **2** a la suma
- El bit de lectura añade **4** a la suma.

Estos valores nunca producen combinaciones ambiguas y cada una representa un conjunto de permisos específicos. De modo tal puede considerarse la siguiente tabla:

Valor	Permiso	Descripción
0	---	Nada
1	--x	Sólo ejecución de archivos o acceso a directorios
2	-w-	Sólo escritura
3	-wx	Escritura y ejecución de archivos o acceso a directorios
4	r--	Sólo lectura
5	r-x	Lectura y ejecución de archivos o acceso a directorios
6	rw-	Lectura y escritura
7	rwx	Lectura, escritura y ejecución de archivos o acceso a directorios

Cabe señalar que el permiso 3 (wx) es el resultado de 1+2 (w+x), que el permiso 5 (rx) es el resultado de 4+1 (r+x), que el permiso 6 (rw) es el resultado de 4+2 (r+w) y que el permiso 7 (rwx) es el resultado de 4+2+1 (r+w+x).

25.3.1. Máscara de usuario.

La máscara de usuario (*umask*, abreviatura de ***u**ser **mask***) es una función que establece los permisos predeterminados para los nuevos archivos y directorios creados en el sistema. Puede establecerse en notación octal de tres o cuatro dígitos o bien en notación simbólica. Puede establecerse cualquier valor para *umask*, pero debe tomarse en consideración que ésta jamás permitirá crear nuevos archivos ejecutables.

Cuando se utiliza la notación octal de cuatro dígitos, el primer dígito siempre corresponde a los permisos especiales, pero el valor de éste siempre será 0; el segundo dígito corresponde a la máscara de la clase otros; el tercer dígito corresponde a la máscara para la clase de grupo; y el cuarto dígito corresponde a la máscara para la clase de usuario.

```
.----------- Permisos especiales (siempre es 0 en umask)
| .--------- Clase de otros
| | .------- Clase de grupo
| | | .----- Clase de usuario
| | | |
↓ ↓ ↓ ↓
0 0 2 2
```

El valor de la máscara de usuario, que se asigna con el mandato **umask**, corresponde a los bits contrarios del permiso predeterminado que se quiera asignar. Es decir, si por ejemplo se quiere asignar una máscara de usuario equivalente a 0775 (rwxrwxr-x), el valor de la máscara de usuario corresponderá a 0002 (el resultado de la operación 777 menos 775), que será lo mismo que definir u=rwx,g=rwx,o=rx.

Si por ejemplo se quiere asignar una máscara de usuario equivalente a 0744 (rwxr--r--), el valor de la máscara de usuario corresponderá a 0033 (el resultado de la operación 777 menos 744), que será lo mismo que definir u=rwx,g=r,o=r.

Los valores nunca producen combinaciones ambiguas y cada una representa un conjunto de permisos específicos. De modo tal puede considerarse la siguiente tabla:

Valor octal	Valor simbólico	Descripción
0	rwx	Lectura, escritura y acceso a directorios
1	rw-	Lectura y escritura
2	r-x	Lectura y acceso a directorios
3	r--	Sólo lectura
4	-wx	Escritura y acceso a directorios
5	-w-	Sólo escritura
6	--x	Sólo acceso a directorios
7	---	Nada

El valor predeterminado de la máscara de usuario del sistema en CentOS, Fedora™, Red Hat™ Enterprise Linux, openSUSE™ y SUSE™ Linux Enterprise es **0022**, es decir se asigna permiso 0755 (-rwxr-xr-x) para nuevos directorios y 0644 (-rw-r--r--) para nuevos archivos. El sistema jamás permite crear nuevos archivos con atributos de ejecución. El valor predeterminado se define en una variable de entorno del archivo **/etc/profile** y puede ser cambiado por el que el administrador del sistema considere pertinente. El valor también puede establecerse por usuario en el archivo **~/.bash_profile** (CentOS, Fedora™ y Red Hat™ Enterprise Linux) o bien en el archivo **~/.profile** (openSUSE™ y SUSE™ Linux Enterprise).

El valor predeterminado de la máscara de usuario utilizado por el mandato **useradd**, para la creación de directorios de inicio de usuarios, se define en el archivo **/etc/login.defs**.

En CentOS, Fedora™ y Red Hat™ Enterprise Linux el valor predeterminado de la máscara de usuario utilizada por el mandato **useradd** es 0077, es decir que los directorios de inicio de cada usuario que sea creado en el sistema tendrá un permiso 0700 (rwx------).

En openSUSE™ y SUSE™ Linux Enterprise el valor predeterminado de la máscara de usuario utilizada por el mandato **useradd** es 0022, es decir 0755 (rwxr-xr-x), debido a que la variable **UMASK** está deshabilitada con una almohadilla en el archivo **/etc/login.defs**, pues se recomienda se defina ésta variable en el archivo **/etc/default/useradd**. Ejemplo:

```
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
CREATE_MAIL_SPOOL=yes
UMASK=0077
```

Para determinar el valor en notación octal para la máscara de usuario predeterminada del sistema, ejecute el mandato **umask**, sin opciones ni argumentos.

```
umask
```

Para determinar el valor en notación simbólica para la máscara de usuario predeterminada del sistema, ejecute el mandato **umask** con la opción **-S** (mayúscula), sin argumentos.

```
umask -S
```

Para cambiar la mascara de usuario en la sesión activa y procesos hijos, se requiere ejecutar el mandato **umask** con el valor octal deseado. En el siguiente ejemplo, se definirá 0002 (0775, rwxrwxr-x) como máscara de usuario:

```
umask 0002
```

Lo anterior también se puede hacer utilizando notación simbólica:

```
umask u=rwx,g=rwx,o=rx
```

25.3.2. Permisos adicionales.

Hay una forma de cuatro dígitos. Bajo este esquema el estándar de tres dígitos descrito arriba se convierte en los últimos tres dígitos del conjunto. El primer dígito representa el bit de los permisos adicionales. En sistemas y equipamiento lógico donde es obligatorio incluir este primer dígito del conjunto de cuatro y se prescinde de asignar permisos adicionales, se debe establecer cero como valor de éste. Ejemplo:

```
chmod 0755 /lo/que/sea
```

El primer dígito del conjunto de cuatro es también la suma de sus bits que le componen:

1. El *bit pegajoso* (*sticky bit*) añade **1** al total de la suma.
2. El bit *setgid* añade **2** al total de la suma.
3. El bit *setuid* añade **4** al total de la suma.

El permiso SUID o bit *setuid* hace que cuando se ha establecido ejecución, el proceso resultante asumirá la identidad del usuario dado en la clase de usuario (propietario del elemento).

El permiso SGID o bit *setgid* hace que cuando se ha establecido ejecución, el proceso resultante asumirá la identidad del grupo dado en la clase de grupo (propietario del elemento). Cuando *setgid* ha sido aplicado a un directorio, todos los nuevos archivos creados debajo de este directorio heredarán el grupo propietario de este mismo directorio. Cuando se omite establecer *setgid*, el comportamiento predeterminado es asignar el mismo grupo del usuario utilizado para crear nuevos archivos o directorios.

El *bit pegajoso* (*sticky bit*) significa que un usuario sólo podrá modificar y eliminar archivos y directorios subordinados dentro de un directorio que le pertenezca. En ausencia de éste, se aplican las reglas generales y el derecho de acceso de escritura en si sólo permite al usuario crear, modificar y eliminar archivos y directorios subordinados dentro de un directorio. Los directorios a los cuales se les ha establecido *bit pegajoso* restringen las modificaciones de los usuarios a sólo adjuntar contenido, manteniendo control total sobre sus propios archivos y permitiendo crear nuevos archivos; sólo permitirá adjuntar o añadir contenido a los archivos de otros usuarios. El *bit pegajoso* es utilizado en directorios como **/tmp** y **/var/spool/mail**.

De modo tal puede considerarse la siguiente tabla:

Valor	Permiso	Descripción
1	`--- --- --t`	*bit pegajoso*
2	`--- --s ---`	bit setgid
3	`--- --s --t`	*bit pegajoso* + bit setgid
4	`--s --- ---`	bit setuid
5	`--s --- --t`	bit *setuid* + *bit pegajoso*
6	`--s --s ---`	bit *setuid* + bit setgid
7	`--s --s --t`	bit *setuid* + bit *setgid* + *bit pegajoso*

Cuando un archivo carece de permisos de ejecución o bien si un directorio carece de permiso de acceso en alguna de las clases y se le es asignado un permiso especial, éste se representa con una letra mayúscula.

Permiso	Clase	Ejecuta	Sin ejecución
setuid	Usuario	s	S
setgid	Grupo	s	S
pegajoso (sticky)	Otros	t	T

25.4. Ejemplos.

25.4.1. Ejemplos permisos regulares.

Valor octal	Valor umask	Clase de Usuario	Clase de Grupo	Clase de Otros
0400	0377	r--	---	---
0440	0337	r--	r--	---
0444	0333	r--	r--	r--
0500	0277	r-x	---	---
0550	0227	r-x	r-x	---
0555	0222	r-x	r-x	r-x
0644	0133	rw-	r--	r--
0664	0113	rw-	rw-	r--
0666	0111	rw-	rw-	rw-
0700	0077	rwx	---	---
0711	0066	rwx	--x	--x
0707	0070	rwx	---	rwx
0744	0033	rwx	r--	r--
0750	0027	rwx	r-x	---
0755	0022	rwx	r-x	r-x
0775	0002	rwx	rwx	r-x
0777	0000	rwx	rwx	rwx

25.4.2. Ejemplos permisos especiales.

Valor octal	Clase de Usuario	Clase de Grupo	Clase de Otros
1644	rw-	r--	r-**T**
2644	rw-	r-**S**	r--
3644	rw-	r-**S**	r-**T**
4644	rw**S**	r--	r--
5644	rw**S**	r--	r-**T**
6644	rw**S**	r-**S**	r--
7644	rw**S**	r-**S**	r-**T**
1777	rwx	rwx	rw**t**
2755	rwx	r-**s**	r-x
3755	rwx	r-**s**	r-**t**
4755	rw**s**	r-x	r-x
5755	rw**s**	r-x	r-**t**
6755	rw**s**	r-**s**	r-x
7755	rw**s**	r-**s**	r-**t**

25.5. Uso del mandato chmod.

```
chmod [opciones] modo archivo
```

Ejecute todos los mandatos del siguiente ejemplo:

```
mkdir -p ~/tmp/
touch ~/tmp/algo.txt
ls -l ~/tmp/algo.txt
chmod 755 ~/tmp/algo.txt
ls -l ~/tmp/algo.txt
chmod u=rw,g=r,o=r ~/tmp/algo.txt
ls -l ~/tmp/algo.txt
chmod u=rw,g-r,o-r ~/tmp/algo.txt
ls -l ~/tmp/algo.txt
chmod u+x,g+rx,o+rx ~/tmp/algo.txt
ls -l ~/tmp/algo.txt
chmod a-x ~/tmp/algo.txt
ls -l ~/tmp/algo.txt
chmod a-w ~/tmp/algo.txt
ls -l ~/tmp/algo.txt
```

La salida debe ser similar a la siguiente:

```
[fulano@localhost ~]$ mkdir -p ~/tmp/
[fulano@localhost ~]$ touch ~/tmp/algo.txt
[fulano@localhost ~]$ ls -l ~/tmp/algo.txt
-rw-rw-r-- 1 fulano fulano 0 ago 18 10:20 /home/fulano/tmp/algo.txt
[fulano@localhost ~]$ chmod 755 ~/tmp/algo.txt
[fulano@localhost ~]$ ls -l ~/tmp/algo.txt
-rwxr-xr-x 1 fulano fulano 0 ago 18 10:20 /home/fulano/tmp/algo.txt
[fulano@localhost ~]$ chmod u=rw,g=r,o=r ~/tmp/algo.txt
[fulano@localhost ~]$ ls -l ~/tmp/algo.txt
-rw-r--r-- 1 fulano fulano 0 ago 18 10:20 /home/fulano/tmp/algo.txt
[fulano@localhost ~]$ chmod u=rw,g-r,o-r ~/tmp/algo.txt
[fulano@localhost ~]$ ls -l ~/tmp/algo.txt
-rw------- 1 fulano fulano 0 ago 18 10:20 /home/fulano/tmp/algo.txt
[fulano@localhost ~]$ chmod u+x,g+rx,o+rx ~/tmp/algo.txt
[fulano@localhost ~]$ ls -l ~/tmp/algo.txt
-rwxr-xr-x 1 fulano fulano 0 ago 18 10:20 /home/fulano/tmp/algo.txt
[fulano@localhost ~]$ chmod a-x ~/tmp/algo.txt
[fulano@localhost ~]$ ls -l ~/tmp/algo.txt
-rw-r--r-- 1 fulano fulano 0 ago 18 10:20 /home/fulano/tmp/algo.txt
[fulano@localhost ~]$ chmod a-w ~/tmp/algo.txt
[fulano@localhost ~]$ ls -l ~/tmp/algo.txt
-r--r--r-- 1 fulano fulano 0 ago 18 10:20 /home/fulano/tmp/algo.txt
[fulano@localhost ~]$
[fulano@localhost ~]$
```

25.5.1. Opciones del mandato chmod.

-R

Cambia permisos de forma descendente en un directorio dado. Es la única opción de los estándares POSIX.

-c

Muestra cuáles archivos han cambiado recientemente en una ubicación dada

-f

Omite mostrar errores de archivos o directorios que haya sido imposible cambiar

-v

Descripción detallada de los mensajes generados por el proceso

Para obtener una descripción completa del uso del mandato **chmod**, ejecute:

```
man 1 chmod
```

25.5.2. El mandato chmod y los enlaces simbólicos.

Cabe señalar que aunque es posible cambiar con los mandatos **chown** y **chgrp** el propietario y/o grupo al cual pertenece un enlace simbólico, el mandato **chmod** jamás cambia los permisos de acceso de enlaces simbólicos, los cuales de cualquier forma carecen de relevancia pues los que importan son los permisos de los archivos o directorios hacia los cuales apuntan. Si se aplica el mandato **chmod** sobre un enlace simbólico, invariablemente se cambiará el permiso del archivo o directorio hacia el cual apunta. Cuando se aplica **chmod** de forma descendente en un directorio, éste ignora los enlaces simbólicos que pudiera encontrar en el recorrido.

Por favor, continué con el documento titulado «***Listas de control de acceso y uso de los mandatos getfacl y setfacl***.»

26. Listas de control de acceso y uso de los mandatos getfacl y setfacl

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

26.1. Introducción.

Los procedimientos de este documento requieren haber estudiado y comprendido previamente los conceptos del documento titulado «***Permisos del sistema de archivos***.»

Este documento describe el uso de listas de control de acceso (**ACL**, ***a****ccess* ***c****ontrol* ***l****ists*), que se utilizan para controlar los permisos de acceso de los archivos y directorios con mayor exactitud. Cada objeto del sistema puede ser asociado a una **ACL** que controla el acceso de modo discrecional hacia ese objeto. Además, los directorios pueden tener asociado un **ACL** que controla los permisos de acceso iniciales para los objetos creados en el interior de éste, a los que se le denomina **ACL** predeterminado.

En resumen, cuando el sistema de archivos ha sido montado con la opción **acl**, es posible asignar permisos de lectura, escritura y ejecución por usuarios y/o grupos. El soporte necesario viene habilitado de modo predeterminado en CentOS, Fedora™, Red Hat™ Enterprise Linux, openSUSE™ y SUSE™ Linux Enterprise 11.

Nota.

En el caso de SUSE™ Linux Enterprise 10, se requiere añadir la opción **acl** en la columna de opciones de la configuración de los sistemas de archivos presentes en el sistema, editando el archivo **/etc/fstab**:

```
vi /etc/fstab
```

Ejemplo:

```
/dev/sda1  /      ext3  acl,user_xattr  1 2
/dev/sda2  /home  ext3  acl,user_xattr  1 2
/dev/sda3  /var   ext3  acl,user_xattr  1 2
```

Para aplicar los cambios de manera inmediata, sin necesidad de reiniciar, se ejecutaría:

```
mount -o remount,acl,user_xattr /
mount -o remount,acl,user_xattr /home
mount -o remount,acl,user_xattr /var
```

26.2. Equipamiento lógico necesario.

26.2.1. En CentOS, Fedora™ y Red Hat™ Enterprise Linux.

La instalación estándar incluye incluye el paquete el paquete **acl**. Si se realiza una instalación mínima, es necesario ejecutar lo siguiente:

```
yum -y install acl
```

Si se utiliza Fedora™ se puede instalar además el paquete **eiciel**, el cual permite gestionar de manera gráfica las listas de control de acceso desde el administrador de archivos (Nautilus) del escritorio de GNOME.

```
yum -y install eiciel
```

26.2.2. En openSUSE™ y SUSE™ Enterprise Linux.

La instalación estándar incluye el paquete **acl**. Si se realizó una instalación mínima, es necesario ejecutar lo siguiente:

```
yast -i acl
```

Si se utiliza openSUSE™ 11 o SUSE™ Enterprise Linux 11 y versiones posteriores de éstos, se puede instalar además el paquete **nautilus-eiciel**, el cual permite gestionar de manera gráfica las listas de control de acceso desde el administrador de archivos (Nautilus) del escritorio de GNOME.

```
yast -i nautilus-eiciel
```

26.3. Procedimientos.

Cuando el soporte para listas de control de acceso está habilitado en los sistemas de archivos y el paquete **acl** está instalado, se pueden utilizar los siguientes dos mandatos:

getfacl

Se utiliza para determinar los permisos establecidos en las listas de control de acceso de un archivo o directorio dado.

setfacl

Se utiliza para cambiar los permisos en las listas de control de acceso de un archivo o directorio dado.

Para obtener una descripción completa del uso del mandato **getfacl**, ejecute:

```
man 1 getfacl
```

Para obtener una descripción completa del uso del mandato **setfacl**, ejecute:

```
man 1 setfacl
```

Para obtener una descripción completa del formato de las listas de control de acceso, ejecute:

```
man 5 acl
```

Para obtener los atributos de las listas de control de acceso de un archivo o directorio particular, se ejecuta el mandato **getfacl** con la ruta del archivo o directorio como argumento. Ejemplo:

```
getfacl /home/fulano
```

Lo anterior devolvería una salida similar la siguiente:

```
getfacl: Eliminando '/' inicial en nombres de ruta absolutos
# file: home/fulano
# owner: fulano
# group: fulano
user::rwx
group::---
other::---
```

Lo anterior muestra que sólo el propietario del directorio tiene permisos de lectura, escritura y acceso.

Para lograr que un usuario en particular pueda acceder también a este directorio, se ejecuta el mandato **setfacl**, con la opción **-m** para modificar la lista de control de acceso, [u,g,o]:[usuario,grupo]:[r,w,x] y la ruta del directorio como argumentos. Ejemplo:

```
setfacl -m u:zutano:rX /home/fulano
```

En el ejemplo anterior se utilizó X mayúscula para indicar que sólo se aplicará el bit de acceso de a directorios evitando aplicar el bit de ejecución a los archivos.

Nota.

Si lo prefiere, también pude utilizar notación octal:

```
setfacl -m u:zutano:5 /home/fulano
```

Lo anterior establece que se añaden permisos de lectura y acceso al directorio /home/fulano para el usuario zutano.

Para verificar, ejecute de nuevo el mandato **getfacl** con la ruta del directorio modificado como argumento:

```
getfacl /home/fulano
```

Lo anterior devolvería una salida similar a la siguiente:

```
getfacl: Eliminando '/' inicial en nombres de ruta absolutos
# file: home/fulano
# owner: fulano
# group: fulano
user::rwx
user:zutano:r-x
group::---
mask::r-x
other::---
```

Pueden asignarse permisos diferentes para otros usuarios. Ejemplo:

```
setfacl -m u:perengano:rwX /home/fulano
```

Lo anterior establece que se añaden permisos de lectura, escritura y acceso al directorio /home/fulano para el usuario perengano. Si utiliza X mayúscula se indicará que se trata específicamente del bit de acceso en lugar de acceso y ejecución.

Para verificar lo anterior, se ejecuta de nuevo el mandato **getfacl** con la ruta del directorio modificado como argumento:

```
getfacl /home/fulano
```

Lo anterior devolvería una salida similar a la siguiente:

```
getfacl: Eliminando '/' inicial en nombres de ruta absolutos
# file: home/fulano
# owner: fulano
# group: fulano
user::rwx
user:perengano:rwx
user:zutano:r-x
group::---
mask::rwx
other::---
```

Estos permisos que se establecieron en la lista de control de acceso del directorio **/home/fulano** son exclusivamente para éste. Cualquier nuevo archivo o directorio creado carecerá de estos nuevos permisos. Si se desea que éstos permisos se vuelvan los predeterminados para los nuevos archivos y directorios que sean creados en lo sucesivo dentro del directorio /home/fulano, se ejecuta el mismo mandato **setfacl**, pero añadiendo la opción **-d** para definir que serán los permisos predeterminados para nuevos archivos y directorios. Ejemplo:

```
setfacl -d -m u:zutano:rX /home/fulano
setfacl -d -m u:perengano:rwX /home/fulano
```

Se recomienda utilizar X mayúscula para indicar que sólo se aplicará el bit de acceso de a directorios evitando aplicar el bit de ejecución a los archivos.

Nota.
Lo anterior también se puede hacer en notación octal:

```
setfacl -d -m u:zutano:5 /home/fulano
setfacl -d -m u:perengano:7 /home/fulano
```

Y la opción **-d** también se puede integrar a los argumentos:

```
setfacl -m d:u:zutano:5 /home/fulano
setfacl -m d:u:perengano:7 /home/fulano
```

Y además simplificar estos últimos dos mandatos en un único mandato:

```
setfacl -m d:u:zutano:5,d:u:perengano:7 /home/fulano
```

Para verificar todo lo anterior, se ejecuta de nuevo el mandato **getfacl** con la ruta del directorio modificado como argumento:

```
getfacl /home/fulano
```

Lo anterior devolvería una salida similar a la siguiente:

```
getfacl: Eliminando '/' inicial en nombres de ruta absolutos
# file: home/fulano
# owner: fulano
# group: fulano
user::rwx
user:perengano:rwx
user:zutano:r-x
group::---
mask::rwx
other::---
default:user::rwx
default:user:perengano:rwx
default:user:zutano:r-x
default:group::---
default:mask::rwx
default:other::---
```

Para aplicar los permisos de forma descendente, se ejecuta el mandato **setfacl** con la opción **-R** (mayúscula), la opción **-m**, [u,g,o]:[usuario,grupo]:[r,w,X,x] y la ruta del directorio como argumento. Ejemplo:

```
setfacl -R -m u:zutano:rX /home/fulano
setfacl -R -m u:perengano:rwX /home/fulano
```

En el ejemplo anterior se utilizó X mayúscula para indicar que sólo se aplicará el bit de acceso de a directorios evitando aplicar el bit de ejecución a los archivos.

Nota.

También puede simplificar estos últimos dos mandatos en un único mandato:

```
setfacl -R -m u:zutano:rX,u:perengano:rwX /home/fulano
```

En el ejemplo anterior se utilizó X mayúscula para indicar que sólo se aplicará el bit de acceso de a directorios evitando aplicar el bit de ejecución a los archivos.

Lo anterior asignaría permisos **r-x** para el usuario zutano y **rwx** para el usuario perengano sobre el directorio **/home/fulano y todo su contenido, pero aplicando sólo el bit de acceso a directorios y evitando asignar bit de ejecución a los archivos.**

Para eliminar los permisos de un usuario en particular de la lista de control de acceso de un directorio en particular, se ejecuta el mandato **setfacl** con la opción **-x**, el nombre del usuario o grupo y la ruta del directorio como argumento. Ejemplo:

```
setfacl -x perengano /home/fulano
```

Para hacer lo mismo, pero de forma descendente, se ejecuta el mandato **setfacl** con la opción **-R** (mayúscula), la opción **-x**, el nombre del usuario o grupo y la ruta del directorio como argumento. Ejemplo:

```
setfacl -R -x perengano /home/fulano
```

Para eliminar los permisos predeterminados en la lista de control de acceso, se ejecuta el mandato **setfacl** con la opción **-k** (--remove-default) y la ruta del directorio como argumento. Ejemplo:

```
setfacl -k /home/fulano
```

Para eliminar todos los permisos en la lista de control de acceso, dejando todo como en el punto inicial, se ejecuta el mandato **setfacl** con la opción **-b** (--remove-all) y la ruta del directorio como argumento. Ejemplo:

```
setfacl -b /home/fulano
```

Para hacer lo mismo, pero de forma descendente, se ejecuta el mandato **setfacl** con la opción **-R** (mayúscula), la opción **-b** (--remove-all) y la ruta del directorio como argumento. Ejemplo:

```
setfacl -R -b /home/fulano
```

Para copiar la lista de control de acceso de un archivo y aplicarla en otro, se ejecuta:

```
getfacl archivo1 | setfacl --set-file=- archivo2
```

Para copiar la lista de control de acceso principal como la lista de control de acceso predeterminada, se ejecuta:

```
getfacl --access /home/fulano | setfacl -d -M- /home/fulano
```

27. Uso del mandato chattr.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

27.1. Introducción.

27.1.1. Acerca del mandato chattr.

El mandato **chattr** se utiliza para cambiar los atributos de los sistemas de archivos **ext2**,**ext3** y **ext4**. Desde cierto punto de vista, es análogo al mandato **chmod**, pero con diferente sintaxis y opciones. Utilizado adecuadamente, dificulta las acciones en el sistema de archivos por parte de un intruso que haya logrado suficientes privilegios en un sistema.

En la mayoría de los casos, cuando un intruso consigue suficientes privilegios en un sistema, lo primero que hará será eliminar los registros de sus actividades modificando estructuras de los archivos de bitácoras del sistema y otros componentes. Utilizar el mandato **chattr** ciertamente no es obstáculo para un usuario experto, pero, afortunadamente, la gran mayoría de los intrusos potenciales no suelen ser expertos en GNU/Linux o Unix, dependiendo enormemente de diversos programas o guiones (los denominados *rootkits* y *zappers*) para eliminar aquello que permita descubrir sus actividades.

Utilizar el mandato **chattr**, incluido en el paquete **e2fsprogs**, que se instala de forma predeterminada en todas las distribuciones de GNU/Linux por tratarse de un componente esencial, hace más difícil borrar o alterar bitácoras, archivos de configuración y componentes del sistema. Theodore Ts'o es el desarrollador y quien se encarga de mantener **e2fsprogs**, mismo que se distribuye bajo los términos de la licencia **GNU/GPL**, e incluye otras herramientas como e2fsck, e2label, fsck.ext2, fsck.ext3, fsck.ext4, mkfs.ext2, mkfs.ext3, mkfs.ext4, tune2fs y dumpe2fs, entre muchas otras.

El manual con la descripción completa del uso del mandato **chattr** puede consultarse ejecutando lo siguiente:

```
man 1 chattr
```

URL: http://e2fsprogs.sourceforge.net/

27.2. Opciones.

-R	Cambia de manera descendente los atributos de directorios y sus contenidos. Los enlaces simbólicos que se encuentren, son ignorado
-V	Salida de **charttr** más descriptiva, mostrando además la versión del programa.
-v	Ver el número de versión del programa.

27.3. Operadores.

+	Hace que se añadan los atributos especificados a los atributos existentes de un archivo.
-	Hace que se eliminen los atributos especificados de los atributos existentes de un archivo
=	Hace que se reemplacen los atributos existentes por los atributos especificados.

27.4. Atributos.

A	Establece que la fecha del último acceso (*atime*) no se modifica.
a	Establece que el archivo sólo se puede abrir en modo de adjuntar para escritura.
c	Establece que el archivo es comprimido automáticamente en el disco por el núcleo del sistema operativo. Al realizar lectura de este archivo, se descomprimen los datos. La escritura de dicho archivo comprime los datos antes de almacenarlos en el disco.
D	Cuando se trata de un directorio, establece que los datos se escriben de forma sincrónica en el disco. Es decir, los datos se escriben inmediatamente en lugar de esperar la operación correspondiente del sistema operativo. Es equivalente a la opción **dirsync** del mandato **mount**, pero aplicada a un subconjunto de archivos.
d	Establece que el archivo no sea candidato para respaldo al utilizar la herramienta **dump**.
e	Indica que el archivo o directorio utiliza extensiones (*extents*) para la cartografía de bloques en la unidad de almacenamiento, particularmente de sistemas de archivos Ext4. El mandato **chattr** es incapaz de eliminar este atributo.
i	Establece que el archivo será inmutable. Es decir, se impide que el archivo sea eliminado, renombrado, que se pueden apuntar enlaces simbólicos hacia éste o escribir datos en el archivo.
j	En los sistemas de archivos ext3 y ext4, cuando se montan con las opciones **data=ordered** o **data=writeback**, se establece que el archivo será escrito en el registro por diario (**Journal**). Si el sistema de archivos se monta con la opción **data=journal** (opción predeterminada), todo el sistema de archivos se escribe en el registro por diario y por lo tanto el atributo no tiene efecto.
s	Cuando un archivo tiene este atributo, los bloques utilizados en el disco duro son escritos con ceros, de modo que los datos no se puedan recuperar por medio alguno. Es la forma más segura de eliminar datos.
S	Cuando el archivo tiene este atributo, sus cambios son escritos de forma sincrónica en el disco duro. Es decir, los datos se escriben inmediatamente en lugar de esperar la operación correspondiente del sistema operativo. Es equivalente a la opción **sync** del mandato **mount**.
u	Cuando un archivo con este atributo es eliminado, sus contenidos son guardados permitiendo recuperar el archivo con herramientas para tal fin.

27.5. Uso del mandato chattr.

```
chattr [-RV] +-=[AacDdijsSu] [-v versión] archivos
```

27.5.1. Ejemplos.

el siguiente mandato agrega el atributo inmutable al archivo **algo.txt**..

```
chattr +i algo.txt
```

Verifique con el mandato **lsattr** el atributo que ha sido establecido.

```
lsattr algo.txt
```

Si ejecuta lo siguiente:

```
echo "Hola mundo" > algo.txt
```

Lo anterior devolverá un error, puesto que el archivo se ha convertido en inmutable y por lo tanto se impide su modificación.

El siguiente mandato elimina el atributo inmutable al archivo **algo.txt**.

```
chattr -i algo.txt
```

Verifique con el mandato **lsattr** que se ha eliminado el atributo.

```
lsattr algo.txt
```

El siguiente mandato agrega el modo de *sólo adjuntar* para escritura al archivo **algo.txt**.

```
chattr +a algo.txt
```

Verifique con el mandato **lsattr** el atributo que ha sido establecido.

```
lsattr algo.txt
```

Si ejecuta lo siguiente:

```
echo "Hola mundo" > algo.txt
```

Al igual que con el atributo **i**, será imposible reemplazar contenido. Sin embargo, si ejecuta lo siguiente:

```
echo "Hola mundo" >> algo.txt
```

Se permitirá añadir datos al archivo **algo.txt**.

El siguiente mandato elimina el modo de sólo adjuntar para escritura al archivo **algo.txt**.

```
chattr -a algo.txt
```

Verifique con el mandato **lsattr** que se ha eliminado el atributo.

```
lsattr algo.txt
```

Si se tiene un sistema de archivos Ext3, el siguiente mandato establece que el archivo **algo.txt** sólo tendrá los atributos **a**, **A**, **s** y **S**.

```
chattr =aAsS algo.txt
```

En sistemas de archivos Ext4, lo anterior siempre fallará porque es imposible eliminar el atributo **e** con el mandato **chattr**. En su lugar, ejecute lo siguiente:

```
chattr =eaAsS algo.txt
```

Verifique con el mandato **lsattr** los atributos que han sido establecidos.

```
lsattr algo.txt
```

28. Uso del mandato rpm.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales (incluyendo su publicación, a través de cualquier medio, por entidades con fines de lucro). c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en castellano. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

28.1. Introducción.

28.1.1. Acerca de RPM.

RPM (**R**PM **P**ackage **M**anager, anteriormente conocido como **R**ed Hat **P**ackage**M**anager, es un sistema de gestión de paquetes de equipamiento lógico para GNU/Linux y que está considerado en la Base Estándar para Linux (**L**inux **S**tandard **B**ase o **LSB**), proyecto cuyo objetivo es desarrollar y promover estándares para mejorar la compatibilidad entre las distribuciones de GNU/Linux para permitir a las aplicaciones ser utilizadas en cualquier distribución.

RPM fue originalmente desarrollado por **Red Hat, Inc.** para su distribución de GNU/Linux y ha sido llevado hacia otra distribuciones de GNU/Linux y otros sistemas operativos.

RPM utiliza una base de datos que se almacena dentro del directorio **/var/lib/rpm**, la cual contiene toda la meta-información de todos los paquetes que son instalados en el sistema y que es utilizada para dar seguimiento a todos los componentes que son instalados. Ésto permite instalar y desinstalar limpiamente todo tipo de aplicaciones, programas, bibliotecas compartidas, etc. y gestionar sus dependencias.

El mandato **rpm** viene instalado de modo predeterminado en **CentOS**, **Fedora**, **Red Hat Enterprise Linux** , **SuSE Linux Enterprise**, **openSuSE**, **Mandriva** y las distribuciones derivadas de éstas.

28.2. Procedimientos.

28.2.1. Reconstrucción de la base de datos de RPM.

Hay ciertos escenarios en donde se puede corromper la base de datos de **RPM**, cómo un sector dañado en la unidad de almacenamiento principal. Si el daño en el sistema de archivos lo permite, la base de datos se puede reconstruir fácilmente utilizando el siguiente mandato:

```
rpm --rebuilddb
```

28.2.2. Consulta de paquetes instalados en el sistema.

Si se desea saber si está instalado un paquete en particular, se utiliza el mandato **rpm** con la opción **-q**, que realiza una consulta (*query*) en la base de datos por un nombre de paquete en particular. En el siguiente ejemplo, se utilizará el mandato **rpm** para preguntar a la base de datos si está instalado el paquete **coreutils**:

```
rpm -q coreutils
```

Lo anterior debe devolver una salida similar a la siguiente:

```
coreutils-8.4-16.el6.x86_64
```

Si se desea conocer qué información incluye el paquete **coreutils**, se utiliza el mandato **rpm** con las opciones **-qi**, para hacer la consulta y solicitar información del paquete (*query info*). En el siguiente ejemplo se consulta la información del paquete **coreutils**:

```
rpm -qi coreutils
```

Lo anterior debe devolver una salida similar a la siguiente:

```
Name        : coreutils                    Relocations: (not relocatable)
Version     : 8.4                               Vendor: CentOS
Release     : 16.el6                         Build Date: mié 07 dic 2011 15:54:01 CST
Install Date: jue 17 may 2012 21:27:47 CDT      Build Host: c6b18n2.bsys.dev.centos.org
Group       : System Environment/Base       Source RPM: coreutils-8.4-16.el6.src.rpm
Size        : 12836729                         License: GPLv3+
Signature   : RSA/SHA1, jue 08 dic 2011 13:50:15 CST, Key ID 0946fca2c105b9de
Packager    : CentOS BuildSystem <http://bugs.centos.org>
URL         : http://www.gnu.org/software/coreutils/
Summary     : A set of basic GNU tools commonly used in shell scripts
Description :
These are the GNU core utilities.  This package is the combination of
the old GNU fileutils, sh-utils, and textutils packages.
```

Puede consultarse cuáles componentes forman parte del paquete utilizando el mandato **rpm** con las opciones **-ql**, donde se realiza una consulta listando los componentes que lo integran (*query list*). Como ejemplo, si se desea conocer cuáles archivos instaló el paquete **coreutils**, ejecute el siguiente mandato:

```
rpm -ql coreutils
```

Lo anterior debe devolver una salida muy extensa, similar a la siguiente:

```
/bin/arch
/bin/basename
/bin/cat
/bin/chgrp
/bin/chmod
/bin/chown
/bin/cp
/bin/cut
/bin/date
...
/usr/share/man/man1/users.1.gz
/usr/share/man/man1/vdir.1.gz
/usr/share/man/man1/wc.1.gz
/usr/share/man/man1/who.1.gz
/usr/share/man/man1/whoami.1.gz
/usr/share/man/man1/yes.1.gz
```

Si se desea consultar a cuál paquete pertenece un archivo instalado en el sistema, se utiliza el mandato **rpm** con las opciones **-qf**, que realizan una consulta por un archivo en el sistema de archivos (*query file*). En el siguiente ejemplo se consultará al mandato **rpm** a que paquete pertenece el archivo **/bin/cp**:

```
rpm -qf /bin/cp
```

Lo anterior debe devolver una salida similar a la siguiente:

```
coreutils-8.4-16.el6.x86_64
```

Si desea consultar la lista completa de paquetes instalados en el sistema, utilice el siguiente mandato, donde **-qa** significa consultar todo (*query all*):

```
rpm -qa
```

Debido a que lo anterior devuelve una lista demasiado grande para poderla visualizar con comodidad, puede utilizarse el mandato **less** o bien el mandato **more**, como subrutina:

```
rpm -qa |less
```

Si se quiere localizar un paquete o paquetes en particular, se puede utilizar el mandato **rpm** con las opciones **-qa** y utilizar **grep** como subrutina. En el siguiente ejemplo se hace una consulta donde se quiere conocer que paquetes están instalado en el sistema y que incluyan la cadena **utils** en el nombre.

```
rpm -qa |grep utils
```

Lo anterior pudiera devolver una salida similar a la siguiente:

```
pulseaudio-utils-0.9.21-13.el6.x86_64
libselinux-utils-2.0.94-5.2.el6.x86_64
glx-utils-7.11-3.el6.x86_64
coreutils-8.4-16.el6.x86_64
xorg-x11-server-utils-7.5-5.2.el6.x86_64
pciutils-3.1.4-11.el6.x86_64
binutils-2.20.51.0.2-5.28.el6.x86_64
nfs-utils-lib-1.1.5-4.el6.x86_64
...
sg3_utils-libs-1.28-4.el6.x86_64
alsa-utils-1.0.21-3.el6.x86_64
db4-utils-4.7.25-16.el6.x86_64
keyutils-libs-1.4-3.el6.x86_64
pciutils-libs-3.1.4-11.el6.x86_64
desktop-file-utils-0.15-9.el6.x86_64
xorg-x11-xkb-utils-7.4-6.el6.x86_64
```

Si se quiere revisar en orden cronológico, de más nuevos a más antiguos, que paquetes están instalados, se puede agregar a **-qa** la opción **--last** y **less** o **more** como subrutina para visualizar con comodidad la salida.

```
rpm -qa --last|less
```

Lo anterior devuelve una salida extensa dentro con **less** como visor. Pulse la teclas de **arriba** (↑) y **abajo** (↓) o **Av. Pág.** y **Reg. Pág.** para desplazarse en la lista. Pulse la tecla **q** para salir.

Si se quiere verificar si los componentes instalados por un paquete **RPM** han sido modificados o alterados o eliminados, se puede utilizar el mandato **rpm** con la opción **-V**, la cual realiza una verificación de la integridad de los componentes de acuerdo a las firmas digitales de cada componente (MD5SUM o suma MD5). En el siguiente ejemplo se verificara si el paquete **cups** ha sido alterado:

```
rpm -V cups
```

Si algún componente fue modificado, puede devolverse una salida similar a la siguiente, donde se indica que el archivo **/etc/cups/printers.conf** fue modificado después de la instalación del paquete cups:

```
S.5....T c /etc/cups/printers.conf
```

Si se desea realizar una verificación de todos los componentes del sistema, se puede utilizar el mandato rpm con las opciones **-Va**, que hace una consulta, especifica todos los paquetes y solicita se verifique si hubo cambios (*query all Verify*).

```
rpm -Va
```

Lo anterior puede devolver una salida muy extensa, pero sin duda alguna mostrará todos los componentes que fueron modificados o alterados o eliminados tras la instalación del paquete al que pertenecen. Un ejemplo de una salida común sería:

```
.......T c /etc/pki/nssdb/cert8.db
.......T c /etc/pki/nssdb/key3.db
..5....T c /etc/pki/nssdb/secmod.db
S.5....T c /etc/crontab
.......T c /etc/inittab
S.5....T c /etc/rc.d/rc.local
S.5....T c /etc/mail/access
S.5....T c /etc/mail/local-host-names
S.5....T c /etc/mail/sendmail.cf
S.5....T c /etc/mail/sendmail.mc
```

28.2.3. Instalación de paquetes.

La mayoría de los distribuidores serios de equipamiento lógico en formato RPM siempre utilizan una firma digital PG/GnuPG (GNU Privacy Guard) para garantizar que éstos son confiables y como un método de evitar que paquetes alterados, generalmente dañados o con malas intenciones, pasen inadvertidamente por los sistemas de gestión de paquetes como yum, zypper, YaST, etc., sin ser detectados. Las firmas digitales de los responsables de la distribución siempre incluyen firmas digitales en el disco de instalación o bien en alguna parte del sistema de archivos. En el caso de **CentOS**, **Fedora** y **Red Hat Enterprise Linux**, las firmas digitales están dentro del directorio /etc/pki/rpm-gpg/. Algunos distribuciones pueden tener estas firmas digitales hospedadas en algún servidor HTTP o FTP. Para importar una firma digital, se utiliza el mandato **rpm** con la opción **--import**. Para ejemplificar, ejecute lo siguiente:

```
rpm --import http://www.alcancelibre.org/al/AL-RPM-KEY
```

Lo anterior importa la firma digital de **Alcance Libre** y permitirá detectar si un paquete de Alcance Libre fue alterado o está corrupto o si fue dañado.

Cuando se instalan paquetes con firma digital validada en el anfitrión local, la salida es similar a la siguiente:

```
Preparando...                ########################################### [100%]
   1:google-chrome-stable    ########################################### [100%]
```

Cuando se instalan paquetes sin firma digital validada en el anfitrión local, la salida es similar a la siguiente:

```
advertencia:google-chrome-stable_current_x86_64.rpm: CabeceraV4
DSA/SHA1 Signature, ID de clave 7fac5991: NOKEY
Preparando...                ########################################### [100%]
   1:google-chrome-stable    ########################################### [100%]
```

Descargue la firma digital de Google, la cual servirá para validar los paquetes para GNU/Linux en formato RPM que distribuye esta compañía:

```
wget https://dl-ssl.google.com/linux/linux_signing_key.pub
```

Importe la firma digital de Google:

```
rpm --import linux_signing_key.pub
```

Cuando se desee instalar un paquete con extensión ***.rpm**, siempre es conveniente revisar dicho paquete. Hay varias formas de verificar su contenido antes de proceder a instalado. Para fines demostrativos, ingrese hacia http://get.adobe.com/es/flashplayer/ y descargue el paquete **flash-plugin-11.2.202.236-release.x86_64.rpm** (o bien el paquete **flash-plugin-11.2.202.236-release.i586.rpm** para sistemas de 32 bit).

Una vez descargado el paquete **flash-plugin**, se puede verificar la información de éste utilizando el mandato **rpm** con las opciones **-qpi** (*query package information*, consultar información del paquete), para realizar la consulta especificando que se trata de un paquete **RPM** en el sistema de archivos.

```
rpm -qpi flash-plugin-11.2.202.236-release.x86_64.rpm
```

Lo anterior debe devolver una salida similar a la siguiente:

```
Name        : flash-plugin                 Relocations: (not relocatable)
Version     : 11.2.202.236                      Vendor: Adobe Systems Inc.
Release     : release                       Build Date: vie 11 may 2012 00:33:53 CDT
Install Date: (not installed)               Build Host: frbld_lnx_024
Group       : Applications/Internet         Source RPM: flash-plugin-11.2.202.236-release.src.rpm
Size        : 20320439                         License: Commercial
Signature   : (none)
Packager    : Adobe Systems Inc.
URL         : http://www.adobe.com/downloads/
Summary     : Adobe Flash Player 11.2
Description :
Adobe Flash Plugin 11.2.202.236
Fully Supported: Mozilla SeaMonkey 1.0+, Firefox 1.5+, Mozilla 1.7.13+
```

Si se desea conocer que componentes va a instalar un paquete **RPM** en particular, se puede utilizar el mandato **rpm** con las opciones **-qpl**, para realizar la consulta, especificar que se trata de un paquete **RPM** y para solicitar la lista de componentes (*query package list*). En el siguiente ejemplo se realiza esta consulta contra el paquete **flash-plugin-11.2.202.236-release.x86_64.rpm**:

```
rpm -qpl flash-plugin-11.2.202.236-release.x86_64.rpm
```

Lo anterior debe devolver una salida similar a la siguiente:

```
/usr/bin/flash-player-properties
/usr/lib64/flash-plugin
/usr/lib64/flash-plugin/LICENSE
/usr/lib64/flash-plugin/README
/usr/lib64/flash-plugin/homecleanup
/usr/lib64/flash-plugin/libflashplayer.so
/usr/lib64/flash-plugin/setup
/usr/lib64/kde4/kcm_adobe_flash_player.so
/usr/share/applications/flash-player-properties.desktop
/usr/share/doc/flash-plugin-11.2.202.236
/usr/share/doc/flash-plugin-11.2.202.236/readme.txt
/usr/share/icons/hicolor/16x16/apps/flash-player-properties.png
/usr/share/icons/hicolor/22x22/apps/flash-player-properties.png
/usr/share/icons/hicolor/24x24/apps/flash-player-properties.png
/usr/share/icons/hicolor/32x32/apps/flash-player-properties.png
/usr/share/icons/hicolor/48x48/apps/flash-player-properties.png
/usr/share/kde4/services/kcm_adobe_flash_player.desktop
```

Para verificar si las firmas digitales de un paquete **RPM** son las mismas y el paquete está íntegro y sin alteraciones, se puede utilizar el mandato **rpm** con las opción **-K**, que solicita verificar firmas digitales de un paquete **RPM** (*Keys*):

```
rpm -K flash-plugin-11.2.202.236-release.x86_64.rpm
```

Si el paquete está integro, debe devolver una salida similar a la siguiente:

```
flash-plugin-11.2.202.236-release.x86_64.rpm: sha1 md5 BIEN
```

Si el paquete RPM fue dañado, alterado o está corrupto, puede devolver una salida similar a la siguiente:

```
flash-plugin-11.2.202.236-release.x86_64.rpm: (sha1) dsa sha1 MD5 GPG NOT OK
```

Para instalar un paquete, se utiliza el mandato **rpm** con las opciones **-ivh**, que significa instalar, devolver una salida descriptiva y mostrar una barra de progreso (*install verbose hash*). Si el paquete está exento de conflicto con otro y/o respeta sin sobre-escribir componentes de otro paquete, se procederá a instalar el mismo. En el siguiente ejemplo se instalará el paquete **flash-plugin-11.2.202.236-release.x86_64.rpm**:

```
rpm -ivh flash-plugin-11.2.202.236-release.x86_64.rpm
```

Asumiendo que todas las dependencias del paquete **flash-plugin-11.2.202.236-release.x86_64.rpm** están cubiertas, lo anterior debe devolver una salida similar a la siguiente:

```
Preparing...                ########################################### [100%]
1:flash-plugin              ########################################### [100%]
```

Si hubiera una versión de éste paquete instalada en el sistema, **rpm -ivh** no realizará la instalación y devolverá un mensaje respecto a que la está instalado dicho paquete. Repita el siguiente mandato:

```
rpm -ivh flash-plugin-11.2.202.236-release.x86_64.rpm
```

Al ya estar instalado el paquete **flash-plugin**, el sistema deberá devolver una salida similar a la siguiente:

```
Preparing...                ########################################### [100%]
    flash-plugin-11.2.202.236-release.x86_64.rpm is already installed
```

Hay circunstancias y escenarios donde se requiere reinstalar de nuevo el paquete. Para lograr ésto se agrega la opción **--force** para forzar la re-instalación de un paquete. En el siguiente ejemplo se solicita al mandato **rpm** forzar la re-instalación de el paquete **flash-plugin-11.2.202.236-release.x86_64.rpm**:

```
rpm -ivh --force flash-plugin-11.2.202.236-release.x86_64.rpm
```

Lo anterior debe devolver una salida similar a la siguiente:

```
Preparing...                ########################################### [100%]
1:flash-plugin              ########################################### [100%]
```

Para verificar las dependencias de un paquete descargado, se utiliza el mandato **rpm** con las opciones **-qp** y **--requires**, la cual consulta las dependencias del paquete. En el siguiente ejemplo, se consultan las dependencias del paquete **flash-plugin-11.2.202.236-release.x86_64.rpm**:

```
rpm -qp --requires flash-plugin-11.2.202.236-release.x86_64.rpm
```

Lo anterior debe devolver una salida similar a la siguiente:

```
glibc >= 2.4
/bin/sh
/bin/sh
/bin/sh
/bin/sh
rpmlib(PayloadFilesHavePrefix) <= 4.0-1
rpmlib(CompressedFileNames) <= 3.0.4-1
```

Pueden hacerse consultas a la inversa de lo anterior, es decir, consultar al mandato **rpm** que paquete provee alguna dependencia en particular. En el siguiente ejemplo se ejecutará el mandato **rpm** para consultar qué paquete provee la dependencia **/bin/sh**.

```
rpm -q --whatprovides /bin/sh
```

Lo anterior debe devolver una salida similar a la siguiente:

```
bash-4.2.10-4.fc14.al.x86_64
```

También puede consultarse qué requiere de un paquete o componente en particular. En el siguiente ejemplo se consulta al mandato **rpm** que paquetes requieren al paquete **bash**.

```
rpm -q --whatrequires /bin/sh
```

Lo anterior puede devolver una salida similar a la siguiente:

```
rsyslog-4.6.3-3.fc14.x86_64
jline-0.9.94-0.6.fc14.noarch
dracut-009-12.fc14.al.noarch
sendmail-8.14.5-2.fc14.al.2.x86_64
autofs-5.0.5-31.fc14.x86_64
cronie-1.4.8-2.fc14.x86_64
PackageKit-command-not-found-0.6.21-3.fc14.al.x86_64
initscripts-9.20.2-2.fc14.al.1.x86_64
```

De ser necesario, se puede incluso hacer consultas respecto a archivos (como bibliotecas compartidas) para conocer que paquetes dependen de éstos. En el siguiente ejemplo se consulta la mandato **rpm** que paquetes requieren a la biblioteca compartida **libbz2.so.1()(64bit)** (utilice «**libbz2.so.1**» en lugar de «**libbz2.so.1()(64bit)**» en sistemas de 32 bit):

```
rpm -q --whatrequires "libbz2.so.1()(64bit)"
```

Lo anterior debe devolver una salida similar a la siguiente y que consiste en una lista de paquetes **RPM** instalados en el sistema que dependen de la biblioteca compartida **libbz2.so.1()(64bit)** (utilice «**libbz2.so.1**» en lugar de «**libbz2.so.1()(64bit)**» en sistemas de 32 bit):

```
bzip2-libs-1.0.5-7.el6_0.x86_64
bzip2-1.0.5-7.el6_0.x86_64
gnupg2-2.0.14-4.el6.x86_64
deltarpm-3.5-0.5.20090913git.el6.x86_64
python-2.6.6-29.el6.x86_64
libsemanage-2.0.43-4.1.el6.x86_64
rpm-4.8.0-19.el6_2.1.x86_64
rpm-libs-4.8.0-19.el6_2.1.x86_64
rpm-python-4.8.0-19.el6_2.1.x86_64
elinks-0.12-0.20.pre5.el6.x86_64
tokyocabinet-1.4.33-6.el6.x86_64
libarchive-2.8.3-4.el6_2.x86_64
genisoimage-1.1.9-11.el6.x86_64
gnome-vfs2-2.24.2-6.el6.x86_64
libgsf-1.14.15-5.el6.x86_64
gstreamer-plugins-bad-free-0.10.19-2.el6.x86_64
yelp-2.28.1-13.el6_2.x86_64
```

Acceda hacia google.com/chrome y descargue el paquete **google-chrome-stable_current_x86_64.rpm** (o bien descargue el paquete **google-chrome-stable_current_i386.rpm** para sistemas de 32 bit).

Para instalar o actualizar un paquete, se utiliza el mandato **rpm** con las opciones -Uvh, que significa instalar o actualizar, devolver una salida descriptiva y mostrar una barra de progreso (*update, verbose, hash*) y se procede a instalar y/o actualizar el mismo:

```
rpm -Uvh google-chrome-stable_current_x86_64.rpm
```

Si las dependencias necesarias están instaladas en el sistema, la salida será similar la siguiente:

```
Preparando...                ########################################### [100%]
   1:google-chrome-stable    ########################################### [100%]
```

Si faltan dependencias por satisfacer, el sistema devolverá una salida similar a la siguiente:

```
error: Error de dependencias:
         lsb >= 4.0 es necesario por google-chrome-stable-20.0.1132.47-144678.i386
         libatk-1.0.so.0 es necesario por google-chrome-stable-20.0.1132.47-144678.i386
         libgconf-2.so.4 es necesario por google-chrome-stable-20.0.1132.47-144678.i386
         libXss.so.1 es necesario por google-chrome-stable-20.0.1132.47-144678.i386
         libXcomposite.so.1 es necesario por google-chrome-stable-20.0.1132.47-144678.i386
         libXfixes.so.3 es necesario por google-chrome-stable-20.0.1132.47-144678.i386
```

Evidentemente se deben instalar primero los paquetes que cubran las dependencias necesarias para poder instalar el paquete **google-chrome-stable_current_x86_64.rpm**. Los paquetes necesarios pueden estar incluidos en el disco de instalación o bien estar incluidos en los almacenes de paquetería en línea. Salvo que se conozcan los paquetes correspondientes y se desee hacer todo manualmente, lo más recomendable es instalar las dependencias a través de el mandato yum (CentOS, Fedora y Red Hat Enterprise Linux) o bien los mandatos yast o zypper (openSUSE y SUSE Linux Enterprise).

Algunos paquetes incluyen guiones que ejecutan procesos que pueden ser requeridos previo o posterior a la instalación. Si se desea omitir la ejecución de estos guiones, se añade a **rpm -ivh** o **rpm -Uvh** la opción **--noscripts**. En el siguiente ejemplo, se instalará el paquete **google-chrome-stable_current_x86_64.rpm** sin la ejecución de los guiones que pudieran estar definidos dentro del paquete **RPM**:

```
rpm -Uvh --noscripts google-chrome-stable_current_x86_64.rpm
```

28.2.3.1. Recuperación de permisos originales a partir de rpm.

En circunstancias en las cuales se realizaron cambios en los permisos en el sistema de archivos, es posible regresar éstos a los permisos originales de acuerdo a las especificaciones de los paquetes **RPM** involucrados, ejecutando el mandato **rpm** con la opción **--setperms**, como se muestra en el siguiente ejemplo:

```
rpm --setperms paquete
```

Visualice el permiso actual del archivo **/bin/cp** ejecutando lo siguiente:

```
ls -l /bin/cp
```

Lo anterior puede devolver una salida similar a la siguiente:

```
-rwxr-xr-x. 1 root root 116696 dic  7  2011 /bin/cp
```

Cambie el permiso del archivo **/bin/cp** ejecutando lo siguiente:

```
chmod 700 /bin/cp
```

Vuelva a visualizar el permiso del archivo **/bin/cp** ejecutando lo siguiente:

```
ls -l /bin/cp
```

Lo anterior debe devolver una salida similar a la siguiente:

```
-rwx------. 1 root root 116696 dic  7  2011 /bin/cp
```

El archivo **/bin/cp** pertence al paquete coreutils y puede confirmalo ejecutando lo siguiente:

```
rpm -qf /bin/cp
```

Lo anterior debe devolver una salida similar a la siguiente:

```
coreutils-8.4-16.el6.x86_64
```

Una vez que se ha determinado a cuál paquete pertenece, para recuperar el permiso original del archivo **/bin/cp**, ejecute lo siguiente:

```
rpm --setperms coreutils
```

Vuelva a ver el permiso de **/bin/cp** ejecutando lo siguiente:

```
ls -l /bin/cp
```

Lo anterior debe devolver una salida similar a la siguiente y que corresponde al permiso original del archivo **/usr/bin/passwd**:

```
-rwxr-xr-x. 1 root root 116696 dic  7  2011 /bin/cp
```

28.2.4. Desinstalación de paquetes.

Para desinstalar paquetes, se utiliza el mandato **rpm** con la opción -e, que se utiliza para eliminar, seguida del nombre del paquete. En el siguiente ejemplo, se solicita al mandato **rpm** desinstalar los paquetes **nc** y **wget**:

```
rpm -e nc wget
```

Si se carece de dependencias que lo impidan, el sistema sólo devolverá el símbolo de sistema.

Si el paquete o alguno de sus componentes fuera dependencia de otro u otros paquetes, el sistema informará que es imposible desinstalar y devolverá la lista de paquetes que dependen del que se está tratando de desinstalar. En el siguiente ejemplo se intentará desinstalar el paquete **python**:

```
rpm -e python
```

Como el paquete **python** es requerido por muchos otros paquetes instalados en el sistema, éste devolverá una salida similar a la siguiente:

```
error: Error de dependencias:
         python(abi) = 2.6 se necesita para (instalado) python-iniparse-0.3.1-2.1.el6.noarch
         python(abi) = 2.6 se necesita para (instalado) python-pycurl-7.19.0-8.el6.x86_64
         python(abi) = 2.6 se necesita para (instalado) python-urlgrabber-3.9.1-8.el6.noarch
         python(abi) = 2.6 se necesita para (instalado) yum-metadata-parser-1.1.2-16.el6.x86_64
         python(abi) = 2.6 se necesita para (instalado) pygpgme-0.1-18.20090824bzr68.el6.x86_64
         python(abi) = 2.6 se necesita para (instalado) newt-python-0.52.11-3.el6.x86_64
...
         /usr/bin/python se necesita para (instalado) gnome-panel-2.30.2-14.el6.x86_64
         /usr/bin/python se necesita para (instalado) totem-2.28.6-2.el6.x86_64
         /usr/bin/python se necesita para (instalado) system-config-firewall-1.2.27-5.el6.noarch
         /usr/bin/python se necesita para (instalado) redhat-lsb-4.0-3.el6.centos.x86_64
         /usr/bin/python2 se necesita para (instalado) firstboot-1.110.11-1.el6.x86_64
```

Si se desea desinstalar cualquier paquete sin importar que otros dependan de este, se puede utilizar agregar la opción **--nodeps**. Esto es contraindicado y sólo debe ser utilizado en situaciones muy particulares. Evite siempre desinstalar paquetes que sean dependencia de otros en el sistema a menos que vaya a reinstalar inmediatamente un paquete que cubra las dependencias que se hayan visto afectadas.

29. Uso del mandato yum.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

29.1. Introducción

29.1.1. Acerca de YUM.

YUM (**Y**ellow Dog **U**pdater, **M**odified) es una herramienta libre, escrita en Python, diseñada para gestión de paquetes en distribuciones de GNU/Linux que utilizan RPM. Fue desarrollado por Seth Vidal y otros colaboradores y es mantenido actualmente como parte del proyecto Linux@DUKE de la Universidad de Duke. Desde que Seth Vidal trabaja en Red Hat, Inc., programadores de dicha compañía están implicados en el desarrollo de yum y han mejorado mucho su funcionalidad y desempeño.

Actualmente es el gestor de paquetes de facto de CentOS, Fedora y Red Hat Enterprise Linux y otras distribuciones de GNU/Linux basadas sobre éstas.

Actualizar el sistema aplicando los más recientes parches de seguridad y correctivos, es hoy más fácil gracias a YUM. El infierno de resolver dependencias entre paquetes RPM terminó hace muchos años. A continuación, los procedimientos para utilizar yum y **realizar fácilmente** lo que algunos denominan «*horrible, difícil y complicado*.»

29.2. Procedimientos

29.2.1. Listados.

Lo siguiente listará todos los paquetes en la base de datos yum disponibles para instalación :

```
yum list available | less
```

Lo siguiente listará todos los paquetes instalados en el sistema:

```
yum list installed | less
```

Lo siguiente listará sólo las versiones instaladas en el sistema del paquete kernel:

```
yum list installed kernel
```

Lo siguiente listará todos los paquetes instalados en el sistema y que pueden (y deben) actualizarse:

```
yum list updates | less
```

Lo siguiente listará todos los paquetes instalados, disponibles y actualizaciones:

```
yum list all | less
```

Lo siguiente listará sólo los paquetes instalados, disponibles y actualizaciones cuyo nombre coincida con la expresión regular «*tools*»:

```
yum list *tools*
```

Lo siguiente mostrará la lista de todos los grupos de paquetes disponibles en los almacenes YUM:

```
yum grouplist
```

29.2.2. Búsquedas.

Realizar una búsqueda de algún paquete o expresión regular en la base de datos en alguno de los almacenes YUM configurados en el sistema:

```
yum search nombre-paquete
```

Ejemplo:

```
yum search cups
```

29.2.3. Consulta de información

Consultar la información contenida en un paquete en particular::

```
yum info nombre-paquete
```

Ejemplo:

```
yum info cups
```

Consultar la lista de paquetes que conforman un grupo de paquetes en particular:

```
yum groupinfo "Nombre del Grupo"
```

El valor de «*Nombre del Grupo*» es de acuerdo a la lista mostrada por la ejecución del mandato **yum grouplist**.

Ejemplo:

```
yum groupinfo "Servidor Web"
```

29.2.4. Instalación de paquetes

Instalación de paquetes con resolución automática de dependencias, a partir de los almacenes en línea:

```
yum install nombre-paquete
```

Ejemplo:

```
yum install cups-pdf
```

Instalación de paquetes con resolución automática de dependencias, sin verificación de firmas digitales, a partir de los almacenes en línea:

```
yum install --nogpgcheck nombre-paquete
```

Ejemplo:

```
yum install --nogpgcheck cups-pdf
```

Instalación de paquetes con resolución automática de dependencias, a partir de los almacenes en línea, sin dialogo de confirmación:

```
yum -y install nombre-paquete
```

Ejemplo:

```
yum -y install cups-pdf
```

Instalación de paquetes con resolución automática de dependencias, localizados en el sistema de archivos local:

```
yum localinstall ~/Descargas/paquete.rpm
```

Ejemplo:

```
yum localinstall google-chrome-stable_current_x86_64.rpm
```

Instalación de paquetes con resolución automática de dependencias, localizados en el sistema de archivos local, sin dialogo de confirmación:

```
yum -y localinstall ~/Descargas/paquete.rpm
```

Ejemplo:

```
yum -y localinstall google-chrome-stable_current_x86_64.rpm
```

Instalación de paquetes con resolución automática de dependencias, sin verificación de firmas digitales, localizados en el sistema de archivos local:

```
yum localinstall --nopgpcheck ~/Descargas/paquete.rpm
```

Ejemplo:

```
yum localinstall --nopgpcheck \
    google-chrome-stable_current_x86_64.rpm
```

Instalación de grupos de paquetes con resolución automática de dependencias:

```
yum groupinstall "Nombre del Grupo"
```

El valor de «*Nombre del Grupo*» es de acuerdo a la lista mostrada por la ejecución del mandato **yum grouplist**.

Ejemplo:

```
yum groupinstall "Servidor Web"
```

Instalación de grupos de paquetes con resolución automática de dependencias, sin dialogo de confirmación:

```
yum -y groupinstall "Nombre del Grupo"
```

Ejemplo:

```
yum -y groupinstall "Servidor Web"
```

De modo predeterminado, la instalación de grupos sólo incluirá los paquetes obligatorios y los predeterminados. Para instalar los paquetes opcionales, algo poco recomendado, edite el archivo **/etc/yum.conf**:

```
vim /etc/yum.conf
```

Añada la opción **group_package_types** con los valores **default, mandatory, optional**. Ejemplo:

```
[main]
cachedir=/var/cache/yum/$basearch/$releasever
keepcache=0
debuglevel=2
logfile=/var/log/yum.log
exactarch=1
obsoletes=1
gpgcheck=1
plugins=1
installonly_limit=3
group_package_types=default, mandatory, optional

#  This is the default, if you make this bigger yum won't see if the metadata
# is newer on the remote and so you'll "gain" the bandwidth of not having to
# download the new metadata and "pay" for it by yum not having correct
# information.
#  It is esp. important, to have correct metadata, for distributions like
# Fedora which don't keep old packages around. If you don't like this checking
# interupting your command line usage, it's much better to have something
# manually check the metadata once an hour (yum-updatesd will do this).
# metadata_expire=90m

# PUT YOUR REPOS HERE OR IN separate files named file.repo
# in /etc/yum.repos.d
```

29.2.5. Desinstalación de paquetes

Evite utilizar la opción **-y** al desinstalar paquetes, a menos que se esté seguro de las consecuencias. Preferentemente siempre corrobore qué es lo que se va a desinstalar antes de responder **Si** o **Yes**.

Para llevar a cabo la desinstalación de paquetes, junto con todo aquello que dependa de éstos:

```
yum remove nombre-paquete
```

Ejemplo:

```
yum remove cups-pdf
```

Para llevar a cabo la desinstalación de grupos de paquetes con resolución automática de dependencias:

```
yum groupremove "Nombre del Grupo"
```

El valor de «*Nombre del Grupo*» es de acuerdo a la lista mostrada por la ejecución del mandato **yum grouplist**.

Ejemplo:

```
yum groupremove "Servidor Web"
```

29.2.6. Actualizar sistema.

Para llevar a cabo la actualización del sistema, ejecute:

```
yum update
```

Para llevar a cabo la actualización del sistema, sin dialogo de confirmación, ejecute:

```
yum -y update
```

Para llevar a cabo la actualización del sistema, omitiendo los paquetes con dependencias rotas, ejecute:

```
yum --skip-broken update
```

Para llevar a cabo la actualización de un solo paquete del sistema, ejecute:

```
yum update nombre-paquete
```

Ejemplo:

```
yum update cups
```

Para llevar a cabo la actualización de un solo paquete del sistema, sin dialogo de confirmación, ejecute:

```
yum -y update nombre-paquete
```

Ejemplo:

```
yum -y update cups
```

Actualización de grupos de paquetes con resolución automática de dependencias:

```
yum groupupdate "Nombre del Grupo"
```

El valor de «*Nombre del Grupo*» es de acuerdo a la lista mostrada por la ejecución del mandato **yum grouplist**.

Ejemplo:

```
yum groupupdate "Base de datos MySQL"
```

Actualización de grupos de paquetes con resolución automática de dependencias, sin dialogo de confirmación:

```
yum -y groupupdate "Nombre del Grupo"
```

Ejemplo:

```
yum -y groupupdate "Base de datos MySQL"
```

29.2.7. Limpieza del directorio de cache.

Yum deja como resultado de su uso metadatos y paquetes almacenados dentro del directorio **/var/cache/yum/**. Cuando se establece la opción **keepcache=1** en el archivo **/etc/yum.conf**, los paquetes RPM que se han instalado pueden ocupar mucho espacio, por lo cual conviene eliminarlos. De igual modo, periódicamente conviene hacer lo mismo con los metadatos viejos detrás de servidores proxy-cache.

A fin de realizar la limpieza de todo el cache de YUM (metadatos, paquetes, etc.), puede ejecutarse lo siguiente:

```
yum clean all
```

A fin de realizar sólo la limpieza de metadatos, puede ejecutarse lo siguiente:

```
yum clean metadata
```

A fin de realizar sólo la limpieza de paquetes descargados, puede ejecutarse lo siguiente:

```
yum clean packages
```

29.2.8. Verificación de la base de datos RPM.

Para verificar la base de datos de RPM en busca de dependencias rotas, ejecute:

```
yum check
```

30. Configuración y uso de Crond.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales (incluyendo su publicación, a través de cualquier medio, por entidades con fines de lucro). c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en castellano. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

30.1. Introducción.

30.1.1. Acerca del servicio crond.

El servicio **crond** es proporcionado por el paquete **cronie** (utilizado en CentOS 6, Fedora™, openSUSE™ y Red Hat™ Enterprise Linux 6), el cual es un proyecto derivado de **vixie-cron** (utilizado en CentOS 5, Red Hat™ Enterprise Linux 5 y SUSE™ Linux Enterprise 10 y 11) y que incluye mejoras en la configuración y en la seguridad, como la capacidad de utilizar PAM y SELinux.

Crond es un servicio del sistema encargado de ejecutar mandatos en horarios determinados. Los mandatos programados pueden definirse en el archivo de configuración **/etc/crontab**. Se puede utilizar además el directorio **/etc/cron.d**, el cual sirve para almacenar archivos con el mismo formato del archivo **/etc/crontab**.

El sistema dispone además de varios directorios utilizados por el servicio crond:

- **/etc/cron.daily**: todo lo que se coloque dentro de este directorios, se ejecutará una vez todos los días.
- **/etc/cron.weekly**: todo lo que se coloque dentro de este directorios, se ejecutará una vez cada semana.
- **/etc/cron.monthly**: todo lo que se coloque dentro de este directorios, se ejecutará una vez al mes.

Los archivos contenidos en estos directorios sólo puede ser modificados por **root** y pueden incluir archivos ejecutables con algún programa en BASH o mandatos particulares.

El servicio utiliza también archivos localizados dentro del directorio **/var/spool/cron**, que son generados por los usuarios regulares a través del mandato **crontab** con la opción **-e** y que permiten a éstos el poder programar mandatos.

De modo predeterminado, todos los usuarios con intérprete de mandatos pueden utilizar el servicio **crond**, a través del mandato **crontab** y programar, en los horarios que sean necesarios, los mandatos a los que se tengan privilegios. Es posible restringir el uso de este servicio, añadiendo la lista de nombres de los usuarios a los cuales se requiera denegar el uso de éste, dentro del archivo **/etc/cron.deny** (un nombre de usuario por renglón).

El paquete correspondiente al servicio **crond** incluye diferentes manuales que describen el uso y configuración. Para obtener una descripción detallada del uso del mandato **crontab**, ejecute **man 1 crontab**:

```
man 1 crontab
```

Para obtener una descripción detallada del formato utilizado para definir las fechas a utilizar y una descripción detallada de la configuración del archivo **/etc/crontab** y el formato a seguir para los archivos que se almacenen dentro de los directorios de configuración mencionados, ejecute **man 5 crontab**:

```
man 5 crontab
```

30.2. Equipamiento lógico necesario.

De modo predeterminado, tras ser instalado, el servicio **crond** viene habilitado en los niveles de ejecución 2, 3, 4 y 5 y seguramente estará en ejecución.

Salvo que se haya hecho algún cambio en el archivo **/etc/sysconfig/crond**, como por ejemplo para añadir algún argumento al inicio del servicio, es innecesario reiniciar el servicio. La ejecución de los mandatos programados se realiza procesando el contenido de los archivos y directorios de configuración.

30.2.1. En CentOS, Fedora™ y Red Hat™ Enterprise Linux.

Si utiliza **CentOS 6** o **Red Hat™ Enterprise Linux 6** o versiones posteriores de éstos, el paquete **cronie** se incluye en la instalación predeterminada. De ser necesario, ejecute lo siguiente para instalar el paquete **cronie**:

```
yum -y install cronie
```

Si utiliza **CentOS 5** o **Red Hat™ Enterprise Linux 5**, éstos sistemas operativos utilizan el paquete **vixie-cron**, el cual se incluye en la instalación predeterminada. De ser necesario, ejecute lo siguiente para instalar el paquete **vixie-cron**:

```
yum -y install vixie-cron
```

Para iniciar el servicio por primera vez cuando recién se ha instalado **cronie**, sólo ejecute:

```
service crond start
```

30.2.2. En openSUSE™.

El paquete **cronie** se incluye en la instalación predeterminada de openSUSE™. Si fuese necesario, instale el paquete **cronie** ejecutando lo siguiente:

```
yast -i cronie
```

Para iniciar el servicio por primera vez cuando recién se ha instalado **cronie**, sólo ejecute:

```
rccron start
```

30.2.3. SUSE™ Linux Enterprise.

El paquete **cron** (alias **vixie-cron**) se incluye en la instalación predeterminada de SUSE™ Linux Enterprise. Si fuese necesario, instale el paquete **cron** ejecutando lo siguiente:

```
yast -i cron
```

Para iniciar el servicio por primera vez cuando recién se ha instalado **cronie**, sólo ejecute:

```
rccron start
```

30.2.4. Anacron.

Para los sistemas donde es imposible que el servicio **crond** se ejecute las 24 horas, los 365 días del año, como ocurre en los equipos portátiles y sistemas de escritorio, conviene instalar además el paquete **cronie-anacron**, el cual se encarga de ejecutar los mandatos programados pendientes que haya sido imposible procesar con el servicio **crond**, al estar éstos configurados en horarios en los cuales esté apagado o suspendido el sistema.

Cabe señalar que **anacron** depende de **cronie** o **vixie-cron**, según corresponda la versión del sistema operativo.

30.2.4.1. Instalación en CentOS, Fedora™ y Red Hat™ Enterprise Linux.

Si utiliza CentOS 6, Fedora™ o Red Hat™ Enterprise Linux 6, instale el paquete **cronie-anacron**, ejecute lo siguiente:

```
yum -y install cronie-anacron
```

Anacron se instala como un mandato programado cada hora.

Si utiliza CentOS 5 o Red Hat™ Enterprise Linux 5, instale el paquete **anacron**, ejecute lo siguiente:

```
yum -y install anacron
```

Si utiliza CentOS 5 o Red Hat™ Enterprise Linux 5, el servicio **anacron** viene activo en los niveles de ejecución 2, 3, 4 y 5. Para iniciarlo por primera vez, ejecute lo siguiente:

```
service anacron start
```

30.2.4.2. Instalación en openSUSE™.

Para instalar **anacron**, ejecute lo siguiente:

```
yast -i cronie-anacron
```

Anacron se instala como un mandato programado cada hora.

30.3. Procedimientos.

30.3.1. Formato para el archivo /etc/crontab.

Cualquier usuario que sea definido para ejecutar un mandato programado en el archivo **/etc/crontab**, podrá ejecutar todo aquello para lo cual tenga privilegios, siempre y cuando se defina un intérprete de mandatos válido (por ejemplo **/bin/bash** o **/bin/sh**) en la variable de entorno **SHELL**, así como las rutas de binarios ejecutables que sean necesarias, sin importar lo que esté definido en el archivo **/etc/passwd** o las variables de entorno definidas en el archivo **~/.bashrc** del usuario a utilizar.

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
```

El archivo **/etc/crontab** permite además definir a cuál usuario enviar un mensaje de correo electrónico con los resultados de las salidas de los mandatos que las generen y el intérprete de mandatos a utilizar.

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=alguien@gmail.com
```

El archivo utiliza un formato de 7 campos, donde se define, respectivamente, minuto, hora, día del mes, mes, día de la semana, usuario a utilizar y el mandato a ejecutar

```
.-----------------------· Minuto (0 - 59)
|  .--------------------· Hora (0 - 23)
|  |  .------------------· Día del mes (1 - 31)
|  |  |  .---------------· Mes (1 - 12)
|  |  |  |  .------------· Día de la semana (0 - 6) (domingo=0 o 7), y
|  |  |  |  |             también acepta como valores:
|  |  |  |  |             mon, tue, wed, thu, fri, sat y sun
|  |  |  |  |  .---------· Usuario
|  |  |  |  |  |      .-· Mandato a ejecutar
↓  ↓  ↓  ↓  ↓  ↓      ↓
1 14  *  *  *  fulano /home/fulano/bin/tarea.sh > /dev/null 2>&1
```

30.3.1.1. Formato exclusivo de cronie.

A diferencia de **vixie-cron**, con **cronie** se pueden omitir los primeras 5 campos y en su lugar utilizar las siguientes opciones:

- @reboot (ejecutar una vez después de reiniciar el sistema)
- @yearly y @annually (ejecutar anualmente, es decir: «`0 0 1 1 *`»)
- @monthly (ejecutar mensualmente, es decir: «`0 0 1 * *`»)
- @weekly (ejecutar semanalmente, es decir: «`0 0 * * 0`»)
- @daily (ejecutar diariamente, es decir: «`0 0 * * *`»)
- @hourly (ejecutar cada hora, es decir: «`0 * * * *`»)

Formato para utilizar con el mandato crontab -e.

Todos los usuarios del sistema pueden ejecutar el mandato **crontab** con la opción **-e**, a excepción de aquellos quienes tengan **/dev/null** (dispositivo nulo) como intérprete de mandatos o bien que se encuentren listados en el archivo **/etc/cron.deny**.

Para los usuarios que tengan **/sbin/nologin** como intérprete de mandatos, será necesario se defina **/bin/bash** o **/bin/sh** en la variable de entorno **SHELL** al inicio del archivo cron correspondiente. Con este tipo de usuarios, habría que ejecutar lo siguiente para poder hacer uso del mandato **crontab**.

```
su -l usuario -s /bin/bash -c "crontab -e"
```

El formato para los usuarios, utilizando el mandato **crontab** con la opción **-e**, es el mismo que el del archivo **/etc/crontab**, pero descartando la columna que define al usuario.

```
.----------------------· Minuto (0 - 59)
|  .-------------------· Hora (0 - 23)
|  |  .-----------------· Día del mes (1 - 31)
|  |  |  .--------------· Mes (1 - 12)
|  |  |  |  .-----------· Día de la semana (0 - 6) (domingo=0 o 7), y
|  |  |  |  |            también acepta como valores:
|  |  |  |  |            mon, tue, wed, thu, fri, sat y sun
|  |  |  |  |  .--------· Mandato a ejecutar
↓  ↓  ↓  ↓  ↓  ↓
1 14  *  *  *  /home/fulano/bin/tarea.sh > /dev/null 2>&1
```

Todos los archivos de cron generados por los usuarios se almacenan siempre dentro del directorio **/var/spool/cron**, utilizando el mismo nombre del usuario como nombre de archivo. Es decir, los mandatos programados por el usuario fulano, se almacenarán en el archivo **/var/spool/cron/fulano**.

30.3.2. Ejemplos de configuraciones.

Considerando el siguiente ejemplo:

```
1  1  *  *  *  root  freshclam > /dev/null 2>&1
```

Lo anterior significa que a las **01:01**, todos los días, todos los meses, todos los años, todos los días de la semana, se ejecutará, como el usuario **root**, el mandato **freshclam**. Se añade al final «**> /dev/null 2>&1**» para que cualquier dato generado por la ejecución de este mandato, se descarte y sea enviando al dispositivo nulo del sistema (**/dev/null**) y que también se envíe la salida de **STDERR** hacia **STDOUT**.

Considerando el siguiente ejemplo:

```
0 23  *  *  5  root  yum -y update > /dev/null 2>&1
```

Lo anterior significa que a las **23:00**, todos los viernes, todos los meses, todos años, se ejecutará, como el usuario **root**, el mandato **yum -y update**. Al igual que en el ejemplo anterior, se añade al final «**> /dev/null 2>&1**» para que cualquier dato generado por la ejecución de este mandato, se descarte y sea enviando al dispositivo nulo del sistema (**/dev/null**) y que también cambie el direccionamiento de **STDERR** hacia **STDOUT**.

Considerando el siguiente ejemplo:

```
*/5 *  *  *  *  root  /sbin/service httpd reload > /dev/null 2>&1
```

Lo anterior significa que cada 5 minutos se ejecutará, como el usuario **root**, el mandato **/sbin/service httpd reload**.

Considerando el siguiente ejemplo:

```
*  */3  *  *  *  root  /sbin/service httpd reload > /dev/null 2>&1
```

Lo anterior significa que cada 3 horas se ejecutará, como el usuario **root**, el mandato **/sbin/service httpd reload**.

Considerando el siguiente ejemplo:

```
*  *  */3  *  *  root  /sbin/service httpd reload > /dev/null 2>&1
```

Lo anterior significa que cada 3 días se ejecutará, como el usuario **root**, el mandato **/sbin/service httpd reload**.

Considerando el siguiente ejemplo:

```
30  10 20  2  *  fulano  wall "¡Feliz cumpleaños a mi!"
```

Lo anterior significa que a las **10:30**, cada **20 de febrero**, todos lo años, se ejecutará, como el usuario **fulano**, el mandato **wall "¡Feliz cumpleaños a mi!"**.

Considerando el siguiente ejemplo:

```
@reboot  fulano  mail -s "El sistema ha reiniciado" alguien@gmail.com
```

Lo anterior significa que cada vez que se reinicie el sistema, se ejecutará, como el usuario **fulano**, el mandato **mail -s "El sistema ha reiniciado"**, mismo que enviará con mensaje de correo electrónico a **alguien@gmail.com**, con el asunto **"El sistema ha reiniciado"**.

31. Configuración y uso de Atd.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales (incluyendo su publicación, a través de cualquier medio, por entidades con fines de lucro). c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en castellano. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

31.1. Introducción.

31.1.1. Acerca de los mandatos at y batch.

Los mandatos **at** y **batch** se utilizan sólo para programar la ejecución de mandatos de una sola ocasión. En el caso de que se requiera programar mandatos para ser ejecutados periódicamente, se sugiere hacerlo a través de crontab.

Ambos mandatos interpretan otros mandatos directamente desde la entrada estándar (STDIN) o a partir de un archivo especificado. El mandato **at** permite especificar que un mandato sea ejecutado a una hora y fecha específicos. El mandato **batch** ejecuta los mandatos sólo cuando descienden los niveles de carga de trabajo del sistema hasta un nivel en particular. Ambos mandatos utilizan el intérprete de mandatos del sistema.

31.2. Equipamiento lógico necesario.

De modo predeterminado el servicio **atd** viene habilitado en los niveles de ejecución 2, 3, 4 y 5 y seguramente estará en ejecución.

Salvo que se haya hecho algún cambio en el archivo **/etc/sysconfig/atd**, como por ejemplo para añadir algún argumento al inicio del servicio, es innecesario reiniciar el servicio. La ejecución de los mandatos programados se realiza procesando el contenido de los archivos y directorios de configuración

31.2.1. En CentOS, Fedora™ y Red Hat™ Enterprise Linux.

Si utiliza **CentOS** o **Red Hat™ Enterprise Linux**, el paquete **at** se incluye en la instalación predeterminada. De ser necesario, ejecute lo siguiente para instalar el paquete **at**:

```
yum -y install at
```

Para iniciar el servicio por primera vez, en caso de que recién se haya instalado **atd**, ejecute:

```
service atd start
```

31.2.2. En openSUSE™ y SUSE™ Linux Enterprise.

El paquete **at** se incluye en la instalación predeterminada de openSUSE™. Si fuese necesario, instale el paquete **at** ejecutando lo siguiente:

```
yast -i at
```

Para iniciar el servicio por primera vez, en caso de que recién se haya instalado **at**, ejecute:

```
rcat start
```

31.3. Procedimientos.

31.3.1. Archivos de configuración /etc/at.allow y /etc/at.deny.

El archivo **/etc/at.deny** se utiliza para definir una lista de usuarios a los cuales se les denegará el uso del mandato **at**. Cuando este archivo está vacío, implica que todos los usuarios del sistema pueden hacer uso del mandato **at**.

El archivo **/etc/at.allow** es inexistente de modo predeterminado. Cuando éste existe, sólo los usuarios listados en su interior pueden hacer uso del mandato **at**.

En ausencia del archivo **/etc/at.allow**, el sistema utilizará siempre **/etc/at.deny** para el control de acceso al mandato **at**.

En ausencia de los archivos **/etc/at.allow** y **/etc/at.deny**, sólo el usuario root puede hacer uso del mandato **at**.

31.3.2. Directorio /var/spool/at.

Todos los mandatos programados con los mandatos **at** y **batch** se almacenan dentro del directorio **/var/spool/at**.

31.3.3. Mandato at.

El mandato **at** se utiliza para ejecutar mandatos a una determinada hora y fecha.

El mandato **at** acepta horas en el formato **HH:MM**. Cuando se ejecuta con una hora que ya ha pasado, el sistema asume que se refiere al día siguiente. También se pueden especificar valores como *midnight* (media noche, 00:00), *noon* (12:00) o *teatime* (16:00). Ejemplo:

```
at 17:30
```

Para especificar la fecha se utiliza el formato nombre-del-mes día, siempre y cuando se especifique después de la hora de ejecución. Ejemplo:

```
at 18:20 Sep 27
```

Opcionalmente también se puede definir el año. Ejemplo:

```
at 18:20 Sep 27 2014
```

También se puede especificar en el formato **MMDDAAAA**, **MM/DD/AAAA** o **DD.MM.AAAA**. Ejemplos:

```
at 10:30 01152015
at 10:30 01/15/2015
at 10:30 15.01.2015
```

Los tres ejemplos anteriores ejecuta un mandato el 15 de enero de 2015 a las 10:30 AM.

También es posible utilizar una hora específica y establecer si se ejecuta ahora (now) más unidades de tiempo, como horas (*hurs*), días (*days*) y semanas (*weeks*). Ejemplo:

```
at 10:30 now + 15 days
```

Lo anterior establece se ejecute un mandato a las 10:30 AM dentro de 15 días.

```
at 10:30 now + 6 weeks
```

Lo anterior establece se ejecute un mandato a las 10:30 AM dentro de 6 semanas.

También permite establecer la ejecución utilizando today (hoy) y tomorrow (mañana) como argumentos. Ejemplo

```
at 12:25 tomorrow
```

El formato completo para la definición de tiempo se puede consultar examinando el contenido del archivo **/usr/doc/at/timespec**.

Una vez que se ejecuta el mandato **at** con alguna hora en particular, se escribe en pantalla el mandato o conjunto de mandato deseados. Para guardar el mandato y salir del intérprete de mandatos del mandato **at**, pulse CTRL-D.

Utilizando la opción **-f** se puede utilizar un archivo específico en lugar de la entrada estándar.

```
at 10:30 today -f /home/usuario/bin/trabajo.sh
```

Que es lo mismo que ejecutar lo siguiente:

```
at 10:30 today < /home/usuario/bin/trabajo.sh
```

El manual completo del mandato **at** puede consultarse ejecutando lo siguiente:

```
man 1 at
```

31.3.4. Mandato batch.

El mandato **batch** se utiliza para ejecutar mandatos cuando el nivel de carga del sistema cae por debajo de 0.8, o bien el valor que se especifique con el mandato **atrun**. El mandato **batch** prescinde del uso de argumentos y sólo permite el uso de la opción **-f** para definir el nombre de un archivo para ser utilizado en lugar de la salida estándar. Ejemplo:

```
batch -f /home/usuario/bin/trabajo.sh
```

Lo anterior es lo mismo que ejecutar lo siguiente:

```
batch < /home/usuario/bin/trabajo.sh
```

Para cambiar el valor de la carga máximo para poder ejecutar los mandatos programados con el mandato batch, se ejecuta el mandato **atrun** con la opción **-l** y el valor de carga deseado. Ejemplo:

```
atrun -l 0.9
```

31.3.5. Mandato atq.

El mandato **atq** muestra una lista de todos los mandatos pendientes. Cuando se ejecuta como usuario regular, muestra exclusivamente los mandatos pendientes de ese usuario en particular. Ejemplo:

```
atq
```

La salida de lo anterior —cuando hay mandatos pendientes— puede ser similar a la siguiente.

```
7       Tue Sep 25 14:30:00 2012 a fulano
5       Thu Jan 15 10:30:00 2015 a fulano
8       Wed Sep 26 14:30:00 2012 a root
6       Thu Jan 15 10:30:00 2015 a zutano
```

El mandato **atq** es en realidad un atajo del siguiente mandato:

```
at -l
```

Cuando se ejecuta como root, muestra todos los mandatos pendientes de todos los usuarios.

31.3.6. Mandato atrm.

El mandato **atrm** se utiliza para eliminar mandatos pendientes, utilizando el número de mandato como argumento. Ejemplo:

```
atrm 2
```

Lo anterior es lo mismo que ejecutar lo siguiente:

```
at -d 2
```

32. Asignación de cuotas en el sistema de archivos.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

32.1. Introducción.

La utilización de cuotas en el sistema de archivos permite a los administradores de sistemas realizar la gestión eficiente del espacio compartido en disco por múltiples usuarios. Las cuotas restringen la capacidad de los usuarios para acceder hacia los recursos de sistema, tales como bloques (asignación de unidades), e inodos (entradas del sistema de archivos). Cuando una cuota es excedida se aplica una política determinada por el administrador. Las cuotas se administran individualmente por cada sistema de archivos y son únicas para usuarios y/o grupos.

32.1.1. Acerca de las cuotas.

Una cuota de disco es un límite establecido por un administrador, el cual restringe ciertos aspectos del uso del sistema de archivos. El objetivo de las cuotas es limitar, de forma razonable, el espacio utilizado en el sistema de archivos. Suelen configurarse en servidores de correo electrónico, servidores HTTP con anfitriones virtuales, servidores de archivos, en algunos sistemas de escritorio y en cualquier escenario donde el administrador del sistema necesite controlar el espacio utilizado por lo usuarios en el sistema de archivos.

32.1.2. Acerca de Inodos.

De acuerdo a Wikipedia, un inodo, nodo-i o también nodo índice, es una estructura de datos propia de los sistemas de archivos en sistemas operativos tipo POSIX (**P**ortable **O**perating **S**ystem **I**nterface for Uni**x**), como GNU/Linux. Un inodo contiene las características (permisos, fechas y ubicación) de un archivo regular, directorio o cualquier otro elemento que pueda contener el sistema de archivos.

Cada inodo queda identificado en el sistema de archivos por un número entero único y los directorios recogen una lista de parejas formadas por un número de inodo y un nombre identificativo que permite acceder a un archivo en particular. Cada archivo tiene un único inodo, pero puede tener más de un nombre en distintos lugares o incluso en el mismo directorio, para facilitar su localización.

32.1.3. Acerca de Bloques.

De acuerdo a Wikipedia, un bloque es la cantidad más pequeña de datos que pueden transferirse en una operación de entrada/salida entre la memoria principal de una computadora y sus dispositivos periféricos o viceversa.

32.2. Equipamiento lógico necesario.

32.2.1. En CentOS, Fedora™ y Red Hat™ Enterprise Linux.

El paquete **quota** viene incluido en la instalación estándar. Si se hizo una instalación mínima, puede instalarse ejecutando lo siguiente:

```
yum -y install quota
```

32.2.2. En openSUSE™ y SUSE™ Enterprise Linux.

El paquete **quota** viene incluido en la instalación estándar de **SUSE™ Linux Enterprise Server**. Si se hizo una instalación mínima o bien se instaló **SUSE™ Linux Enterprise Desktop**, puede instalarse ejecutando lo siguiente:

```
yast -i quota
```

32.3. Procedimientos.

Durante la instalación debió asignarse una partición dedicada para, por mencionar un ejemplo, los directorios **/var** y **/home**.

Edite el archivo **/etc/fstab**.

```
vi /etc/fstab
```

Si utiliza **CentOS 6**, **Fedora™**, **Red Hat™ Enterprise Linux 6** o **SUSE™ Linux Enterprise 11**, puede utilizar cuotas con registro por diario (*journaled quotas*) sin modificar el núcleo del sistema o instalar otra versión de quota-tools. Las cuotas con registro por diario funcionan de modo similar al registro por diario de los sistemas de archivos Ext3/Ext4, garantizando la integridad de los archivos de cuotas, lo cual evita que el sistema se vea obligado a ejecutar automáticamente el mandato **quotacheck** después de un apagado incorrecto.

Añada a la columna de opciones de las particiones **/var** y **/home**, la opción **usrjquota** con el valor **aquota.user**, la opción **grpjquota** con el valor **aquota.group** y la opción **jqfmt** con el valor **vfsv0**:

Si utiliza **CentOS**, **Fedora™** o **Red Hat™ Enterprise Linux**, el siguiente es un ejemplo de cómo pudiera quedar la configuración de las particiones.

```
/dev/sda7  /var   ext4  defaults,usrjquota=aquota.user,grpjquota=aquota.group,jqfmt=vfsv0  1 2
/dev/sda5  /home  ext4  defaults,usrjquota=aquota.user,grpjquota=aquota.group,jqfmt=vfsv0  1 2
```

Si utiliza **openSUSE™** o **SUSE™ Linux Enterprise Linux**, el siguiente es un ejemplo de cómo pudiera quedar la configuración de las particiones.

```
/dev/sda7  /var   ext3  acl,user_xattr,usrjquota=aquota.user,grpjquota=aquota.group,jqfmt=vfsv0  1 2
/dev/sda5  /home  ext3  acl,user_xattr,usrjquota=aquota.user,grpjquota=aquota.group,jqfmt=vfsv0  1 2
```

Nota.

Si utiliza **CentOS 5**, **Red Hat™ Enterprise Linux 5** o **SUSE™ Linux Enterprise 10**, oficialmente éstos carecen de soporte para cuotas con registro por diario. Requieren un parche en el núcleo de Linux para poder hacer uso de éstas. En estos sistemas operativos sólo se pueden utilizar **cuotas sin registro por diario**, por lo cual sólo se deben añadir las opciones **usrquota** y **grpquota** en el archivo **/etc/fstab**, en la columna de opciones correspondientes a las particiones /var y /home. Ejemplo:

```
LABEL=/var      /var    ext3    defaults,usrquota,grpquota      1 2
LABEL=/home     /home   ext3    defaults,usrquota,grpquota      1 2
```

Deben aplicarse los cambios a las particiones, ya sea reiniciando el sistema o bien ejecutando los siguientes mandatos:

```
mount -o remount /var
mount -o remount /home
```

Lo anterior vuelve a leer las opciones de montado de cada una de las particiones y aplicá los cambios inmediatamente.

Ejecute el mandato **quotacheck** con las opciones **-avugcm**, donde **a** significa que se verifican todos los sistemas de archivos con soporte para cuotas, **v** significa que se devuelvan mensajes descriptivos, **u** significa que se verifiquen cuotas de usuario, **g** significa que se verifiquen cuotas de grupo, **c** significa omitir verificar archivos de cuota previos y crear nuevos archivos y **m** significa que se evite re-montar en modo de sólo lectura los sistemas de archivos, que idealmente se utiliza cuando se tiene procesos trabajando en las particiones:

```
quotacheck -avugcm
```

El manual del mandato **quotacheck** puede consultarse ejecutando lo siguiente:

```
man 8 quotacheck
```

Para activar las cuotas recién configuradas, asumiendo que se están configurando las particiones correspondientes a /home y /var, ejecute los siguientes dos mandatos:

```
quotaon /home
quotaon /var
```

32.3.1. Edquota.

El mandato **edquota** se utiliza para gestionar las cuotas asignadas a usuarios y/o grupos. El manual de éste puede consultarse ejecutando lo siguiente:

```
man 8 edquota
```

Es importante conocer que significa cada columna mostrada por el mandato **edquota**.

Blocks: Bloques. Corresponde a la cantidad de bloques de 1 Kb que está utilizando el usuario.

Inodes: Inodos. Corresponde al número de archivos que está utilizando el usuario. Un **inodo** (también conocido como Index Node) es un apuntador hacia sectores específicos en la unidad de almacenamiento en los cuales se encuentra la información de un archivo. Contiene además la información acerca de permisos de acceso así como los usuarios y grupos a los cuales pertenece el archivo.

Soft: Limite de gracia. Limite de bloques de 1 KB o inodos que el usuario tiene permitido utilizar y que puede rebasar hasta que sea excedido el periodo de gracia (de modo predeterminado son 7 días).

Hard: Limite absoluto. Limite que no puede ser rebasado por el usuario bajo circunstancia alguna.

Para asignar cuotas a cualquier usuario regular, se ejecuta el mandato **edquota**, especificando como argumento el nombre del usuario. Ejemplo:

```
edquota fulano
```

Lo anterior deberá devolver algo similar a lo siguiente:

```
Disk quotas for user fulano (uid 501):
Filesystem    blocks     soft     hard   inodes     soft     hard
/dev/sda7          8        0        0        1        0        0
/dev/sda5         24        0        0       10        0        0
```

Para asignar cuotas a cualquier grupo de usuarios regulares, se se ejecuta el mandato **edquota** con la opción **-g**, especificando como argumento el nombre del grupo. Ejemplo:

```
edquota -g desarrollo
```

Lo anterior deberá devolver algo similar a lo siguiente:

```
Disk quotas for group desarrollo (gid 510):
Filesystem    blocks     soft     hard   inodes     soft     hard
/dev/sda7       4238        0        0      251        0        0
/dev/sda5       6234        0        0      340        0        0
```

Cuando se asignan cuotas a grupos, estás definen los límites en conjunto para todo el grupo de usuarios que pertenezcan a un grupo determinado.

32.3.1.1. Cuota absoluta.

Suponiendo que se quiere asignar una cuota de disco de 50 MiB para el usuario «fulano» en en `/dev/sda7` y `/dev/sda5`, se utilizaría lo siguiente:

```
Disk quotas for user fulano (uid 501):
Filesystem    blocks     soft     hard   inodes     soft     hard
/dev/sda7          8        0    51200        1        0        0
/dev/sda5         24        0    51200       10        0        0
```

El usuario siempre podrá rebasar una **cuota de gracia** pero **nunca** una **cuota absoluta**.

32.3.1.2. Cuota de gracia.

De modo predeterminado el sistema asigna un **periodo de gracia** de 7 días, que se puede modificar con el mandato **edquota con la opción -t:**

```
edquota -t
```

Donde se puede establecer un nuevo periodo de gracia, ya sea por días, horas, minutos o segundos.

```
Grace period before enforcing soft limits for users:
Time units may be: days, hours, minutes, or seconds
Filesystem    Block grace period     Inode grace period
/dev/hdb7                 7days                  7days
/dev/hdb5                 7days                  7days
```

La **cuota de gracia** establece los límites de bloques o **inodos** que un usuario tiene en un sistema de archivos en particular. Cuando el usuario excede el límite establecido por la cuota de gracia, el sistema advierte al usuario que se ha excedido la cuota del disco sin embargo permite al usuario continuar escribiendo hasta que trascurre el tiempo establecido por el periodo de gracia, tras el cual al usuario se le impide continuar escribiendo sobre el sistema de archivos. Suponiendo que quiere asignar una cuota de gracia de 25 MiB en `/dev/sda7` y `/dev/sda5`, la cual podrá ser excedida hasta por 7 días, se utilizaría la siguiente configuración:

```
Disk quotas for user fulano (uid 501):
Filesystem    blocks     soft     hard   inodes     soft     hard
/dev/sda7          0    25600        0        0        0        0
/dev/sda5         24    25600        0       10        0        0
```

32.3.1.3. Aplicando cuotas de forma masiva.

Si se quiere aplicar un mismo esuqema de cuotas de disco para todos los usuarios regulares del sistema, a partir de UID 501, por mencionar un ejemplo y asumiendo que utilizará como plantilla el esquema de cuotas de disco del usuario «fulano», ejecute lo siguiente **(note por favor los dos acentos graves en el mandato, pues se trata de un carácter diferente al apostrofe)**:

```
edquota -p fulano `awk -F: '$3 > 501 {print $1}' /etc/passwd`
```

32.4. Comprobaciones.

Utilice como root el mandato **edquota** para modificar los límites del usuario **fulano** ejecutando lo siguiente:

```
edquota fulano
```

Asigne al usuario «fulano» una cuota de gracia de 25 MiB, una cuota absoluta de 50 MiB, un límite de gracia de 1000 archivos y un límite absoluto de 1500 archivos, en todas las particiones con cuota de disco habilitada:

```
Disk quotas for user fulano (uid 501):
Filesystem    blocks     soft     hard   inodes     soft     hard
/dev/sda7          0    25600    51200        0     1000     1500
/dev/sda5         24    25600    51200       10     1000     1500
```

Desde otra terminal o ejecutando **su -l fulano**, acceda hacia el sistema como el usuario fulano o cualquier otro usuario regular existente en el sistema.

El mandato **quota** se utiliza para verificar las cuotas asignadas a usuarios y/o grupos. El manual de éste puede consultarse ejecutando lo siguiente:

```
man 1 quota
```

Cómo usuario regular, ejecute el mandato **quota**:

```
quota
```

Observe con detenimiento la salida:

```
Disk quotas for user fulano (uid 501):
Filesystem  blocks   quota   limit   grace   files   quota   limit   grace
/dev/sda7        8    25600   51200              1    1000    1500
/dev/sda5       24    25600   51200             10    1000    1500
```

Realice una **copia** del directorio **/usr/lib** como el sub-directorio **~/prueba-cuotas** dentro de su directorio de inicio:

```
cp -r /usr/lib ~/prueba-cuotas
```

Notará que llegará un momento en el que el sistema indicará que ya no es posible continuar copiando contenido dentro de **~/prueba-cuotas** debido a que se ha agotado el espacio en el sistema de archivos.

Utilice de nuevo el mandato **quota** y observe con detenimiento la salida, en donde aparecerá un asterisco justo junto a la cantidad en las columnas de bloques y/o inodos, los cuales indican que se han excedido las cuotas:

```
Disk quotas for user fulano (uid 501):
Filesystem  blocks   quota   limit   grace   files   quota   limit   grace
/dev/sda7        8    25600   51200              1    1000    1500
/dev/sda5    51200*   25600   51200   6days   1500*   1000    1500   6days
```

Para poder volver a escribir sobre el sistema de archivos, es necesario liberar espacio. Debido a que muy probablemente parte del contenido de **/usr/lib** se copió en modo de sólo lectura, cambie primero los permisos del contenido del directorio, a fin de disponer de permisos de lectura y escritura:

```
chmod -R u+w ~/prueba-cuotas
```

Elimine el directorio **~/prueba-cuotas**, junto con su contenido:

Y, finalmente, vuelva a ejecutar el mandato **quota**:

```
rm -fr ~/prueba-cuotas
```

Y, finalmente, vuelva a ejecutar el mandato **quota** para verificar que nuevamente se está trabajando dentro de los límites establecidos:

```
quota
```

La salida debe ser nuevamente similar a la siguiente:

```
Disk quotas for user fulano (uid 501):
Filesystem  blocks   quota   limit   grace   files   quota   limit   grace
/dev/sda7        8    25600   51200              1    1000    1500
/dev/sda5       24    25600   51200             10    1000    1500
```

33. Introducción a TCP/IP

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

33.1. Introducción

TCP/IP fue desarrollado y presentado por el Departamento de Defensa de EE.UU. en 1972 y fue aplicado en **ARPANET** (**A**dvanced **R**esearch **P**rojects **A**gency **N**etwork), que era la red de área extensa del Departamento de Defensa como medio de comunicación para los diferentes organismos de EE.UU. La transición hacia TCP/IP en **ARPANET** se concretó en 1983.

Se conoce como **familia de protocolos de Internet** al conjunto de protocolos de red que son implementados por la pila de protocolos sobre los cuales se fundamenta Internet y que permiten la transmisión de datos entre las redes de computadoras.

Los dos protocolos más importantes y que fueron también los primeros en definirse y también los más utilizados, son **TCP** (Protocolo de Control de Transmisión o **T**ransmission **C**ontrol **P**rotocol) e **IP** (Protocolo de Internet o **I**nternet **P**rotocol), de ahí que se denomine también como **Conjunto de Protocolos TCP/IP**. Los tipos de protocolos existentes superan los cien, ente los cuales podemos mencionar como los más conocidos a HTTP, FTP, SMTP, POP, ARP, etc.

TCP/IP es la plataforma que sostiene Internet y que permite la comunicación entre diferentes sistemas operativos en diferentes computadoras, ya sea sobre redes de área local (LAN) o redes de área extensa (WAN).

33.2. Niveles de pila

En la actualidad continúa la discusión respecto a si el modelo TCP/IP de cinco niveles encaja dentro del modelo OSI (Interconexión de Sistemas Abiertos u **O**pen**S**ystems **I**nterconnection) de siete niveles.

Modelo	Niveles
TCP/IP	5 Aplicación 4 Transporte 3 Red 2 Enlace 1 Físico.
OSI	7 Aplicación 6 Presentación 5 Sesión 4 Transporte 3 Red 2 Enlace de datos 1 Físico

33.2.1. Modelo TCP/IP

Utiliza encapsulamiento para proveer la abstracción de protocolos y servicios hacia diferentes capas en la pila. La pila consiste de cinco niveles:

Nivel	Nombre	Descripción
5	**Aplicación**	Se compone de diversos protocolos de servicios como: • **DNS** (Domain Name System) • **TLS/SSL** (**T**ransport **L**ayer **S**ecurity) • **TFTP** (**T**rivial **F**ile **T**ransfer **P**rotocol) • **FTP** (**F**ile **T**ransfer **P**rotocol) • **HTTP** (**H**yper **T**ext **T**ransfer **P**rotocol) • **IMAP** (**I**nternet **M**esssage **A**ccess **P**rotocol) • **IRC** (**I**nternet **R**elay **C**hat) • **NNTP** (**N**etwork **N**ews **T**ransfer **P**rotocol) • **POP3** (**P**ost **O**ffice **P**rotocol) • **SIP** (**S**ession **I**niciation **P**rotocol) • **SMTP** (**S**imple **M**ail **T**ransfer **P**rotocol) • **SNMP** (**S**imple **N**etwork **M**anagement **P**rotcol) • **SSH** (**S**ecure **Sh**ell) • **TELNET** • **BitTorrent** • **RTP** (**R**eal-time **T**ransport **P**rotocol) • **rlogin** • **ENRP** (**E**ndpoint **H**andlespace **R**edundancy **P**rotocol) Los protocolos de encaminamiento como **BGP** (**B**order **G**ateway **P**rotocol) y **RIP** (**R**outing **I**nformation **P**rotocol) que utilizan transporte por TCP y UDP respectivamente pueden ser considerados como parte de este nivel.
4	**Transporte**	Se compone de diversos protocolos de servicios como: • **TCP** (**T**ransmision **C**ontrol **P**rotocol) • **UDP** (**U**ser **D**atagram **P**rotocol), • **DCCP** (**D**atagram **C**ongestion **C**ontrol **P**rotocol) • **SCTP** (**S**tream **C**ontrol **T**ransmision **P**rotococol)

Nivel	Nombre	Descripción
		• **IL** (**I**nternet **L**ink Protocol, similar a TCP pero más simple) • **RUDP** (**R**eliable **U**ser **D**atagram **P**rotocol), etc. Los protocolos como **OSPF** (**O**pen **S**hortest **P**ath **F**irst), que corren sobre IP, pueden ser también considerados como parte de esta capa. **ICMP** (**I**nternet **C**ontrol **M**essage **P**rotocol) e **IGMP** (**I**nternet **G**roup **M**anagement **P**rotocol) que también utilizan IP, pueden ser considerados parte del Nivel de Red.
3	**Red**	Se compone de diversos protocolos de servicios como **IP** (incluyendo **IPv4** e **IPv6**). Protocolos como **ARP** (**A**ddress **R**esolution **P**rotocol) y **RARP** (**R**everse **A**ddress **R**esolution **P**rotocol) que operan por debajo de IP, pero arriba del Nivel de enlace, de modo que pertenecen a un punto intermedio entre el Nivel de Red y el Nivel de Enlace.
2	**Enlace**	Compuesto de protocolos como: • **Ethernet** • **Wi-Fi** • **Token ring** • **PPP** (Point-to-Point **P**rotocol) • **SLIP** (**S**erial **L**ine **I**nternet **P**rotocol) • **FDDI** (Fiber Distributed **D**ata **I**nterface) • **ATM** (**A**synchronous **T**ransfer **P**rotocol) • **Frame Relay** • **SMDS** (Switched **M**ulti-megabit **D**ata **S**ervices)
1	**Físico**	Medio físico.

Los niveles más cercanos altos son los más cercanos al usuario, mientras que los que están más hacia abajo se encuentran más cercanos a la transmisión física de los datos. Salvo por evidentes razones en el primer y último niveles, cada nivel tiene un nivel superior y un nivel inferior que, respectivamente o bien utilizan un servicio del nivel o proveen un servicio. Un método de abstracción para entender esto es mirar los niveles como proveedores o consumidores de servicios. Ejemplo: TCP en el nivel de transporte requiere un protocolo del nivel de Red, como sería IPv4, el cual a su vez requiere de un protocolo del nivel de enlace, siendo TCP un proveedor de servicio para los protocolos del nivel de aplicación.

33.2.1.1. Nivel de aplicación

Es el nivel que utilizan los programas de red más comunes a fin de comunicarse a través de una red. La comunicación que se presenta en este nivel es especifica de las aplicaciones y los datos transportados desde el programa que están en el formato utilizado por la aplicación y van encapsulados en un protocolo del **Nivel de Transporte**. Siendo que el modelo TCP/IP no tiene niveles intermedios, el nivel de Aplicación debe incluir cualquier protocolo que actúe del mismo modo que los protocolos del **Nivel de Presentación** y **Nivel de Sesión** del **Modelo OSI**. Los protocolos del Nivel de Transporte más comúnmente utilizados son TCP y UDP, mismos que requieren un puerto disponible y específico para el servicio para los servidores y puertos efímeros. Aunque los encaminadores (routers) e interruptores (switches) no utilizan este nivel, las aplicaciones que controlan el ancho de banda si lo utilizan.

33.2.1.2. Nivel de Transporte

Este nivel principalmente provee lo necesario para conectar aplicaciones entre si a través de puertos. Mientras que IP (Internet Protocol),del Nivel de Red, provee solamente la mejor forma de entrega, el nivel de transporte es el primer nivel que se encarga de la fiabilidad. De entre todos los protocolos de este nivel, tanto TCP como UDP son utilizados para transportar un gran número de aplicaciones de alto nivel. Las aplicaciones en cualquier nivel se distinguen a través de los puertos TCP o UDP que utilicen.

TCP.

El mejor ejemplo de este nivel es TCP, que es un protocolo orientado hacia conexión que resuelve numerosos problemas de fiabilidad para proveer una transmisión de bytes fiable, ya que se encarga de que los datos lleguen en orden, tenga un mínimo de correcciones de errores, se descarten datos duplicados, se vuelvan a enviar los paquetes perdidos o descartados e incluya control de congestión de tráfico.

La conexiones a través de TCP tienen tres fases:

I. Establecimiento de la conexión

Antes de que el cliente intente conectarse con el servidor, éste último debe primero ligarse hacia el puerto para abrirlo para las conexiones, es decir, una **apertura pasiva**. Una vez establecida, el cliente puede iniciar la **apertura activa**. Se requiere de un saludo de tres etapas:

1. La apertura activa se realiza enviando un paquete SYN (sincroniza) hacia el servidor.
2. En respuesta, el servidor responde con un paquete SYN-ACK (conformación de sincronización).
3. Finalmente el cliente envía un paquete ACK (confirmación) de regreso hacia el servidor.

   En este punto tanto cliente como servidor han recibido una conformación de la conexión.

II. Transferencia de datos

Hay tres funciones clave que diferencian a TCP de UDP:

1. Transferencia de datos libre de errores.
2. Transferencia de datos ordenada.
3. Retransmisión de paquetes perdidos.
4. Descartado de paquetes duplicados.
5. Ajuste en la congestión de la transmisión de datos.

III. **Terminación de la conexión**.

Esta etapa utiliza un saludo de tres vías, con cada extremo de la conexión terminando independientemente. Cuando uno de los extremos desea detener su parte de la conexión, envía un paquete FIN, que la otra parte confirma con un paquete ACK. Por tanto, una interrupción de la conexión requiere un par de paquetes FIN y ACK desde cada lado de la conexión TCP.

Una conexión puede quedar abierta a medias cuando uno de los extremos ha terminado la conexión desde su lado pero el otro extremo no. El extremo que terminó la conexión ya no puede enviar datos en la conexión, pero el el otro extremo sí.

El método más común es un saludo de tres etapas donde un anfitrión A envía un paquete FIN y el anfitrión B responde con un paquete FIN y un ACK (en el mismo paso) y el anfitrión A responde con un paquete ACK.

TCP realiza las siguientes etapas en su zócalo:

1. LISTEN
2. SYN-SENT
3. SYN-RECEIVED
4. ESTABLISHED
5. FIN-WAIT-1
6. FIN-WAIT-2
7. CLOSE-WAIT
8. CLOSING
9. LAST-ACK
10. TIME-WAIT
11. CLOSED

LISTEN representa la conexión en espera de peticiones desde cualquier puerto TCP remoto. **SYN-SENT** representa la espera del TCP remoto para enviar de regreso el paquete TCP estableciendo banderas **SYN** y **ACK**. **SYN-RECIVED** representa la espera para el TCP remoto para enviar de regreso la confirmación después de haber enviado de regreso otra confirmación de conexión al TCP remoto (establecido por el servidor TCP). **ESTABLISHED** representa que el puerto está listo para recibir/enviar datos desde/hacia el TCP remoto (lo hacen tanto clientes como servidores TCP). **TIME-WAIT** representa el tiempo de espera necesario para asegurar que el TCP remoto ha recibido la confirmación de su solicitud de terminación de la conexión.

UDP.

UDP, a veces referido sarcásticamente como *Unreliable* Datagram Protocol (Protcolo no fiable de datagrama), es un protocolo de datagrama sin corrección; no provee las garantía de fiabilidad y ordenamiento de TCP a los protocolos del **Nivel de Aplicación** y los datagramas pueden llegar en desorden o perderse sin notificación. Como consecuencia de lo anterior es que UDP es un protocolo más rápido y eficiente para tareas ligeras o sensibles al tiempo una interfaz muy simple entre el **Nivel de Red** y **Nivel de Aplicación**. Si se requiere algún tipo de fiabilidad para los datos transmitidos, ésta debe ser implementada en los niveles superiores de la pila.

Al igual que IP y a diferencia de TCP, es un protocolo de mejor esfuerzo o no-fiable. El único problema de fiabilidad que resuelve es la corrección de errores en la cabecera y datos transmitidos a través de un campo de 16 bits para **suma de verificación** (checksum), una forma de control de redundancia con la finalidad de proteger la integridad de datos verificando que no hayan sido corrompidos.

La estructura de paquetes UDP consiste de 4 campos.

- **Puerto de origen**. Encargado de identificar el puerto que envía y que se asume será el puerto hacia donde se envía la respuesta si se necesita. Este campo es opcional: si no se utiliza, el valor del campo debe ser 0.
- **Puerto de destino**. Identifica el puerto de destino. Es obligatorio.
- **Longitud**. Un campo de 16 bits que especifica la longitud del datagrama completo: cabecera y datos. La longitud mínima es de 8 bytes ya que es la longitud misma de la cabecera.
- **Suma de verificación**. Un campo de 16 bits que se utiliza para verificar errores en cabecera y datos.

Las aplicaciones más comunes que hacen uso de este tipo de protocolo son DNS, aplicaciones de transmisión de medios, voz sobre IP (VoIP), TFTP y juegos en línea.

SCTP.

SCTP es un **mecanismo de transporte fiable** orientado hacia conexión. Está orientado también hacia transmisión de datos pero no está orientado hacia bytes como TCP. Provee múltiples transmisiones distribuidos sobre una misma conexión. Puede además representar una conexión con múltiples direcciones IP de modo que si una IP falla, la conexión no se interrumpe. Se desarrolló inicialmente para aplicaciones de telefonía pero se puede utilizar en otras aplicaciones.

DCCP.

DCCP se encuentra en fase de desarrollo y bajo la tutela de la IETF (Internet Engineering Task Force) que pretende proveer la semántica de control de flujo de TCP y el modelo de servicio de datagrama de UDP a la vista del usuario.

RTP.

RTP es un protocolo de datagrama que fue diseñado para datos en tiempo real como la transmisión de audio y vídeo. Es un nivel de sesión que utiliza el formato de paquetes de UDP como base. Sin embargo se considera que este protocolo pudiera acomodar debajo del nivel de transporte del modelo TCP/IP.

33.2.1.3. Nivel de Red

Este nivel resuelve el problema de capturar los datos a través de una red única. **IP** (**I**nternet **P**rotocol) realiza la tarea básica de capturar los paquetes de datos desde una fuente hacia un destino. IP puede transportar datos para una gran cantidad de protocolos del nivel superior (Nivel de Transporte). Otro ejemplo de protocolo de este nivel es X.25, que es un conjunto de protocolos para redes WAN utilizando líneas telefónicas o sistema ISDN.

33.2.1.4. Nivel de Enlace

Este nivel no es realmente parte del **Conjunto de Protocolos TCP/IP**, sino que es el método utilizado para pasar paquetes desde el Nivel de Red sobre dos diferentes anfitriones. Este proceso puede ser controlado a través del equipamiento lógico utilizado como controlador del dispositivo para una tarjeta de red así como también sobre la **Programación en firme** (Firmware) o circuitos integrados auxiliares (chipsets). Estos procesos realizarán funciones de enlace de datos tales como añadir una cabecera de paquete para preparar la transmisión y entonces transmitir el todo a través de un medio físico.

Este nivel es donde los paquetes son interceptados y enviados hacia una Red Privada Virtual (VPN). Cuando esto se lleva a acabo, los datos del Nivel de Enlace se consideran como los datos de la aplicación y procede descendiendo por la pila del modelo TCP/IP para realizar la verdadera transmisión. En el extremo receptor, los datos suben por la pila del modelo TCP/IP dos veces, una para la VPN y otra para el encaminamiento (routing).

33.2.1.5. Nivel Físico

Al igual que el Nivel de Enlace, no es realmente parte del **Conjunto de Protocolos TCP/IP**. Contempla todas las características físicas de la comunicación como la naturaleza del medio, detalles de conectores, código de canales y modulación, potencias de señal, longitudes de onda, sincronización y tiempo de vida así como distancias máximas.

33.2.2. Modelo OSI

El **Conjunto de Protocolos TCP/IP** (y su correspondiente pila) han sido utilizados antes de que se estableciera el modelo OSI (Interconexión de Sistemas Abiertos u **O**pen **S**ystems **I**nterconnection) y desde entonces el modelo TCP/IP ha sido comparado con el modelo OSI tanto en libros como en instituciones educativas. Ambas se relacionan pero no son equiparables. El modelo OSI utiliza siete niveles, mientras que el modelo TCP/IP utiliza cinco. Los dos niveles que hacen la diferencia en el Modelo OSI son el **Nivel de Presentación** y el **Nivel de Sesión**, mismos que podrían ser equivalentes al **Nivel de Aplicación** del modelo TCP/IP.

Del mismo modo que la pila del modelo TCP/IP, el modelo OSI no es lo suficientemente diverso en los niveles inferiores para abarcar las verdaderas capacidades del **Conjunto de Protocolos TCP/IP**. Un claro ejemplo es que falta un nivel intermedio para acomodar entre el **Nivel de Red** y el **Nivel de Transporte** para poder determinar donde corresponden los protocolos ICMP e IGMP y otro nivel intermedio entre el **Nivel de Red** y el **Nivel de Transporte** para determinar donde corresponden los protocolos ARP y RARP.

Nivel	Nombre	Descripción
7	**Aplicación**	HTTP, SMTP, SNMP, FTP, Telnet, SIP, SSH, NFS, RTSP, **XMPP** (E**x**tensible **M**essaging and **P**resence **P**rotocol), Whois, ENRP Telnet.
6	**Presentación**	**XDR** (E**x**ternal **D**ata **R**epresentation), **ASN.1** (**A**bstract **S**yntax **N**otation 1), **SMB** (**S**erver **M**essage **B**lock),**AFP** (**A**pple **F**iling **P**rotocol), **NCP** (**N**etWare **C**ore **P**rotocol)
5	**Sesión**	**ASAP** (**A**ggregate **S**erver **A**ccess **P**rotocol), TLS, SSH, ISO 8327 / CCITT X.225, **RPC** (**R**emote **P**rocedure **C**all), **NetBIOS**, **ASP** (**A**ppletalk **S**ession **P**rotocol), Winsock, BSD sockets
4	**Transporte**	TCP, UDP, RTP, SCTP, SPX, ATP, IL
2	**Enlace de datos**	Ethernet, Token ring, HDLC, Frame relay, ISDN, ATM, 802.11 WiFi, FDDI, PPP
1	**Físico**	Define todas las especificaciones físicas y eléctricas de los dispositivos, como son disposición de pines, voltajes, especificaciones de cableado, concentradores, repetidores, adaptadores de red, etc. **Cable**, **Radio**, f**ibra óptica**, **Red por palomas**.

Los niveles 7 al 4 se clasifican como niveles de anfitrión, mientras que los **niveles inferiores** del 1 al 3 se clasifican como **niveles de medios**.

34. Introducción a IP versión 4

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

34.1. Introducción.

IPv4 es la versión 4 del Protocolo de Internet (**IP** o **I**nernet **P**rotocol) y constituye la primera versión de IP que es implementada de forma extensiva. **IPv4** es el principal protocolo utilizado en el Nivel de Red del Modelo TCP/IP para Internet. Fue descrito inicial mente en el RFC 791 elaborado por la Fuerza de Trabajo en Ingeniería de Internet (**IETF** o **I**nternet **E**ngineering **T**ask **F**orce) en Septiembre de 1981, documento que dejó obsoleto al RFC 760 de Enero de 1980.

IPv4 es un protocolo orientado hacia datos que se utiliza para comunicación entre redes a través de interrupciones (switches) de paquetes (por ejemplo a través de Ethernet). Tiene las siguientes características:

- Es un protocolo de un servicio de datagramas no fiable (también referido como de *mejor esfuerzo*).
- No proporciona garantía en la entrega de datos.
- No proporciona ni garantías sobre la corrección de los datos.
- Puede resultar en paquetes duplicado o en desorden.

Todos los problemas mencionados se resuelven en el nivel superior en el modelo TCP/IP, por ejemplo, a través de **TCP** o **UDP**.

El propósito principal de **IP** es proveer una dirección única a cada sistema para asegurar que una computadora en Internet pueda identificar a otra.

34.2. Direcciones.

IPv4 utiliza direcciones de 32 bits (4 bytes) que limita el número de direcciones posibles a utilizar a 4,294,967,295 direcciones únicas. Sin embargo, muchas de estas están reservadas para propósitos especiales como redes privadas, **Multidifusión** (Multicast), etc. Debido a esto se reduce el número de direcciones IP que realmente se pueden utilizar, es esto mismo lo que ha impulsado la creación de **IPv6** (actualmente en desarrollo) como reemplazo eventual dentro de algunos años para **IPv4**.

34.2.1. Representación de las direcciones.

Cuando se escribe una dirección **IPv4** en cadenas, la notación más común es la **decimal con puntos**. Hay otras notaciones basadas sobre los valores de los octetos de la dirección IP.

Utilizando como ejemplo: www.alcancelibre.org que tiene como dirección IP 201.161.1.226 en la notación decimal con puntos:

Notación	Valor	Conversión desde decimal con puntos
Decimal con puntos	201.161.1.226	-
Hexadecimal con puntos	0xC9.0xA1.0x01.0xE2	Cada octeto de la dirección es convertido individualmente a hexadecimal.
Octal con puntos	0311.0241.0001.0342	Cada octeto es convertido individualmente a octal.
Binario con puntos	11001001.10100001.00000001.11100010	Cada octeto es convertido individualmente a binario
Hexadecimal	0xC9A101E2	Concatenación de los octetos de hexadecimal con puntos.
Decimal	3382772194	La forma hexadecimal convertida a decimal.
Octal	31150200742	La forma hexadecimal convertida a octal.
Binario	11001001101000010000000111100010	La forma hexadecimal convertida a binario.

Teóricamente, todos estos formatos mencionados deberían ser reconocidos por los navegadores (sin combinar). Además, en las formas con puntos, cada octeto puede ser representado en combinación de diferentes bases. Ejemplo: 201.0241.0x01.226.

34.3. Asignación

Desde 1993 rige el esquema **CIDR** (**C**lassless **I**nter-**D**omain **R**outing o Encaminamiento Inter-Dominios sin Clases) cuya principal ventaja es permitir la subdivisión de redes y permite las entidades sub-asignar direcciones IP, como haría un ISP con un cliente.

El principio fundamental del encaminamiento (routing) es que la dirección codifica información acerca de localización de un dispositivo dentro de una red. Esto implica que una dirección asignada a una parte de una red no funcionará en otra parte de la red. Existe una estructura jerárquica que se encarga de la asignación de direcciones de Internet alrededor del mundo. Esta estructura fue creada para el **CIDR** y hasta 1998 fue supervisada por la **IANA** (**I**nternet **A**ssigned **N**umbers **A**uthority o Agencia de Asignación de Números Internet) y sus **RIR** (**R**egional **I**nternet **R**egistries o Registros Regionales de Internet). Desde el 18 de Septiembre de 1998 la supervisión está a cargo de la **ICANN** (**I**nternet **C**orporation for **A**ssigned **N**ames and **N**umbers o Corporación de Internet para los Nombres y Números Asignados). Cada **RIR** mantiene una base de datos **WHOIS** disponible al publico y que permite hacer búsquedas que proveen información acerca de las asignaciones de direcciones IP. La información obtenida a partir de estas búsquedas juega un papel central en numerosas herramientas las cuales se utilizan para localizar direcciones IP geográficamente.

34.3.1. Bloques reservados.

Bloques de direcciones reservadas

Bloque de direcciones CIDR	Descripción	Referencia
0.0.0.0/8	Red actual (solo válido como dirección de origen)	RFC 1700
10.0.0.0/8	**Red Privada**	RFC 1918
14.0.0.0/8	Red de datos públicos	RFC 1700
39.0.0.0/8	Reservado	RFC 1797
127.0.0.0/8	Anfitrión local (localhost)	RFC 1700
128.0.0.0/16	Reservado	
169.254.0.0/16	**Red Privada** (Zeroconf)	RFC 3927
172.16.0.0/12	**Red Privada**	RFC 1918

Bloque de direcciones CIDR	Descripción	Referencia
191.255.0.0/16		
192.0.0.0/24		
192.0.2.0/24	Red de pruebas	RFC 3330
192.88.99.0/24	Retransmisión desde **IPv6** hacia **IPv4**	RFC 3068
192.168.0.0/16	**Red Privada**	RFC 1918
198.18.0.0/15	Pruebas de desempeño de red	RFC 2544
223.255.255.0/24	Reservado	RFC 3330
224.0.0.0/4	Multidifusión (Multicast, antes red Clase D)	RFC 3171
240.0.0.0/4	Reservado (Antes red Clase E)	RFC 1700
255.255.255.255	Difusiones (Broadcast)	

34.3.1.1. Redes privadas.

De los más de **cuatro mil millones** de direcciones permitidas por **IPv4**, tres rangos están especialmente reservados para utilizarse solamente en redes privadas. Estos rangos no tienen encaminamiento fuera de una red privada y las máquinas dentro de estas redes privadas no pueden comunicarse directamente con las redes públicas. Pueden, sin embargo, comunicarse hacia redes públicas a través de la Traducción de Direcciones de Red o **NAT** (**N**etwork **A**ddress **T**ranslation).

Bloques reservados para redes privadas

Nombre	Rango de direcciones IP	Numero de direcciones IP	Tipo de clase	Bloque CIDR mayor
Bloque de 24bits	10.0.0.0 – 10.255.255.255	16,777,215	Única clase A	10.0.0.0/8
Bloque de 20bits	172.16.0.0 – 172.31.255.255	1,048,576	16 clases B contiguas	172.16.0.0/12
Bloque de 16bits	192.168.0.0 – 192.168.255.255	65,535	256 clases C contiguas	192.168.0.0/16

34.3.1.2. Anfitrión local (Localhost)

Además de las redes privadas, el rango 127.0.0.0 – 127.255.255.255 o 127.0.0.0/8 en la notación **CIDR**, está reservado para la comunicación del anfitrión local (localhost). Ninguna dirección de este rango deberá aparecer en una red, sea pública o privada y cualquier paquete enviado hacia cualquier dirección de este rango deberá regresar como un paquete entrante hacia la misma máquina.

34.4. Referencia de sub-redes de IP versión 4.

Algunos segmentos del espacio de direcciones de IP, disponibles para la versión 4, se especifican y asignan a través de documentos **RFC** (**R**equest **F**or **C**omments o Solicitud De Comentarios), que son conjuntos de notas técnicas y de organización que se elaboran desde 1969 donde se describen los estándares o recomendaciones de Internet, antes ARPANET. Ejemplos de esto son los usos del Retorno del sistema (loopback, RFC 1643), las redes privadas (RFC 1918) y Zeroconf (RFC 3927) que no están bajo el control de los **RIR** (**R**egional **I**nternet **R**egistries o Registros Regionales de Internet).

La máscara de sub-red es utilizada para separar los bits de un identificados de una red a partir de los bits del identificados del anfitrión. Se escribe utilizando el mismo tipo de notación para escribir direcciones IP.

CIDR	Máscara de sub-red	Anfitriones	Nombre de la clase	Uso típico
/8	255.0.0.0	16777216	Clase A	Bloque más grande definido por la IANA
/9	255.128.0.0	8388608		
/10	255.192.0.0	4194304		
/11	255.224.0.0	2097152		
/12	255.240.0.0	1048576		
/13	255.248.0.0	524288		
/14	255.252.0.0	262144		
/15	255.254.0.0	131072		
/16	255.255.0.0	65536	Clase B	
/17	255.255.128.0	32768		ISP / negocios grandes
/18	255.255.192.0	16384		ISP / negocios grandes
/19	255.255.224.0	8192		ISP / negocios grandes
/20	255.255.240.0	4096		ISP pequeños / negocios grandes
/21	255.255.248.0	2048		ISP pequeños / negocios grandes
/22	255.255.252.0	1024		
/23	255.255.254.0	512		
/24	255.255.255.0	256	Clase C	LAN grande
/25	255.255.255.128	128		LAN grande
/26	255.255.255.192	64		LAN pequeña
/27	255.255.255.224	32		LAN pequeña
/28	255.255.255.240	16		LAN pequeña
/29	255.255.255.248	8		
/30	255.255.255.252	4		Redes de unión (enlaces punto a punto)
/31	255.255.255.254	2		Red no utilizable, sugerida para enlaces punto a punto (RFC 3021)
/32	255.255.255.255	1		Ruta del anfitrión

34.5. Referencias.

- http://www.ietf.org/rfc/rfc760.txt
- http://www.ietf.org/rfc/rfc791.txt
- http://www.ietf.org/rfc/rfc1643.txt
- http://www.ietf.org/rfc/rfc1700.txt
- http://www.ietf.org/rfc/rfc1797.txt
- http://www.ietf.org/rfc/rfc1918.txt
- http://www.ietf.org/rfc/rfc2544.txt
- http://www.ietf.org/rfc/rfc3021.txt
- http://www.ietf.org/rfc/rfc3068.txt
- http://www.ietf.org/rfc/rfc3171.txt
- http://www.ietf.org/rfc/rfc3330.txt
- http://www.ietf.org/rfc/rfc3927.txt

35. Configuración de red en GNU/Linux.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

35.1. Introducción

Configurar los parámetros de red en GNU/Linux requiere se entiendan perfectamente los fundamentos de **IP versión 4** y saber cómo utilizar cualquier editor de texto simple.

En **CentOS** y **Red Hat™ Enterprise Linux**, que utilizan núcleo de Linux versión 2.6, la detección de las tarjetas de red es automática mientras se trate de dispositivos soportados. Para consultar la lista de dispositivos compatibles, visite hardware.redhat.com.

35.2. Procedimientos

35.2.1. Nombres de los dispositivos.

Las más recientes versiones de **CentOS**, **Fedora™** y **Red Hat™ Enterprise Linux** utilizan un nuevo esquema para los nombres de los dispositivos de red. Los nombres se basan sobre su ubicación física con la finalidad de facilitar su identificación. Los dispositivos de red integrados a la tarjeta madre utilizan el esquema **em[1,2,3,4...]**; los dispositivos PCI utilizan el esquema **p[ranura PCI]p[puerto ethernet]** y —en el caso de dispositivos virtuales— **p[ranura PCI]p[puerto ethernet]_[interfaz virtual]**. Ejemplos:

- em1 corresponde al primer dispositivo de red integrado en la tarjeta madre.
- em2 corresponde al segundo dispositivo de red integrado en la tarjeta madre.
- em3 corresponde al tercer dispositivo de red integrado en la tarjeta madre.
- p1p1 corresponde al primer dispositivo de red en la primera ranura PCI, primer puerto ethernet.
- p2p1 corresponde al primer dispositivo de red en la segunda ranura PCI, primer puerto ethernet.
- p3p1 corresponde al primer dispositivo de red en la tercera ranura PCI, primer puerto ethernet.
- p3p2 corresponde al primer dispositivo de red en la tercera ranura PCI, segundo puerto ethernet.
- p3p2_1 corresponde al primer dispositivo de red en la tercera ranura PCI, segundo puerto ethernet, primer dispositivo virtual.

El nuevo esquema de nombres sólo aplica para sistemas que implementan SMBIOS versión 2.6 y tablas 9 y 41. Puede cotejarse la versión de SMBIOS ejecutando como usuario root el siguiente mandato:

```
biosdecode
```

Pueden determinarse los dispositivos de red presentes en el sistema revisando el contenido del directorio **/sys/class/net/**:

```
ls /sys/class/net/
```

Puede consultarse la asignación de nombres de dispositivos de red presentes en el sistema, a través del archivo /etc/udev/rules.d/70-persistent-net.rules.

```
vi /etc/udev/rules.d/70-persistent-net.rules
```

Si se dispone de SMBIOS 2.6 y tablas 41 y 9, para hacer uso del nuevo esquema de nombres en sistemas que fueron actualizados desde una versión anterior de **CentOS**, **Fedora™** y **Red Hat™ Enterprise Linux**, sólo es necesario eliminar este archivo y reiniciar el sistema.

35.2.2. NetworkManager.

A partir de **CentOS 5** y **Red Hat™ Enterprise Linux 5**, se incluye **NetworkManager** como una implementación alternativa para la gestión de parámetros de red desde la interfaz de usuario. En éstos, **NetworkManager** viene desactivado de modo predeterminado.

En **CentOS 6** y **Red Hat™ Enterprise Linux 6**, **NetworkManager** viene activo de modo predeterminado, salvo que se haga la instalación mínima o la instalación básica de servidor.

Si se desea impedir que **NetworkManager** gestione algún dispositivo de red en particular y que éste sea gestionado por el servicio **network**, edite el archivo de configuración correspondiente al dispositivo a utilizar. Asumiendo que se trata del dispositivo eth0, ejecute:

```
vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

Modifique el valor del parámetro **NM_CONTROLLED** y establezca **no** como valor de éste. Ejemplo:

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
HWADDR=44:87:FC:AA:DD:2D
NM_CONTROLLED=no
IPADDR=192.168.70.101
NETMASK=255.255.255.128
GATEWAY=192.168.70.1
DOMAIN=dominio.tld
DNS1=8.8.8.8
DNS2=8.8.4.4
```

Para aplicar los cambios, ejecute lo siguiente:

```
service network restart
```

En adelante, mientras esté establecido **NM_CONTROLLED=no** en la configuración del dispositivo de red, **NetworkManager** ignorará ésta por completo.

Si quiere prescindir del uso de **NetworkManager**, también se puede desactivar por completo este servicio, siendo que su uso sólo tiene sentido en una computadora portátil que se conecta a múltiples redes inalámbricas o bien un sistema escritorio donde se quiere permitir al usuario regular poder controlar los dispositivos de red.

Para desactivar **NetworkManager**, ejecute lo siguiente:

```
chkconfig NetworkManager off
service NetworkManager stop
```

35.2.3. Asignación de parámetros de red.

35.2.3.1. Nombre del anfitrión (HOSTNAME).

Edite el archivo **/etc/hosts**:

```
vi /etc/hosts
```

Respete la configuración de la resolución de retorno del sistema. Añada el nombre de anfitrión del sistema y asocie éste a alguna de las direcciones IP locales. Ejemplo:

```
127.0.0.1       localhost.localdomain   localhost
::1             localhost6.localdomain6 localhost6
192.168.70.101  nombre.dominio.tld      nombre
```

El **nombre del anfitrión** (*hostname*) debe ser un **FQDN** (acrónimo de **F**ully **Q**ualified **D**omain **N**ame o Nombre de Dominio Plenamente Calificado) resuelto por un servidor de nombres de domino (DNS). Puede definir éste editando el archivo **/etc/sysconfig/network**:

```
vi /etc/sysconfig/network
```

Cambie el valor del parámetro HOSTNAME por el nombre de anfitrión que corresponda. Tome en cuenta que el nombre de anfitrión deberá estar resuelto cuando menos en el archivo **/etc/hosts**, y, si es posible, también en un servidor DNS.

```
NETWORKING=yes
HOSTNAME=nombre.dominio.tld
```

A partir de **CentOS 6** y **Red Hat™ Enterprise Linux 6**, el parámetro **HOSTNAME** puede ser establecido en el archivo de configuración de cualquier dispositivo de red del sistema (por ejemplo **/etc/sysconfig/network-scripts/ifcfg-eth0**), en lugar del archivo **/etc/sysconfig/network**.

Asumiendo que se utilizará el dispositivo eth0, edite el archivo **/etc/sysconfig/network-scripts/ifcfg-eth0**:

```
vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

Ejemplo:

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
NM_CONTROLLED=no
IPADDR=192.168.70.101
NETMASK=255.255.255.128
GATEWAY=192.168.70.1
HOSTNAME=nombre.dominio.tld
```

Para aplicar los cambios, ejecute lo siguiente:

```
service network restart
```

35.2.3.2. Dirección IP, máscara de sub-red y puerta de enlace.

Los valores de los parámetros de red se asignan a través de los parámetros **BOOTPROTO** para definir **static** si se utilizará una dirección IP estática o bien **dhcp** si se asignará la dirección IP a través de un servidor DHCP, **IPADDR** para definir la dirección IP, **NETMASK** para definir la máscara de sub-red en formato octal y **GATEWAY** para definir la puerta de enlace.

Asumiendo que se utilizará el dispositivo eth0, edite el archivo **/etc/sysconfig/network-scripts/ifcfg-eth0**:

```
vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

Ejemplo:

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
NM_CONTROLLED=no
IPADDR=192.168.70.101
NETMASK=255.255.255.128
GATEWAY=192.168.70.1
```

En lugar del parámetro NETMASK con un valor octal, puede utilizar el parámetro PREFIX y definir la máscara de sub-red en formato **CIDR**.

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
NM_CONTROLLED=no
IPADDR=192.168.70.101
PREFIX=25
GATEWAY=192.168.70.1
```

Los valores de los parámetros anteriores son proporcionados por el administrador de la red local en donde se localice el sistema que esté siendo configurado o bien definidos de acuerdo a una planificación previamente establecida. El administrador de la red deberá proporcionar una dirección IP disponible (IPADDR) y una máscara de la sub-red (NETMASK o PREFIX).

Para aplicar los cambios, ejecute lo siguiente:

```
service network restart
```

35.2.3.3. Servidores de nombres.

Hay dos parámetros a configurar: dominio de búsqueda predeterminado y al menos un servidor de nombres. En **CentOS 6** y **Red Hat™ Enterprise Linux 6**, se pueden establecer añadiendo al archivo de configuración de cualquier dispositivo de red, los parámetros **DOMAIN**, **DNS1**, **DNS2** y **DNS3**.

Asumiendo que se utilizará el dispositivo eth0, edite el archivo **/etc/sysconfig/network-scripts/ifcfg-eth0**:

```
vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

Ejemplo:

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
NM_CONTROLLED=no
IPADDR=192.168.70.101
PREFIX=25
GATEWAY=192.168.70.1
DOMAIN=dominio.tld
DNS1=8.8.8.8
DNS2=8.8.4.4
```

Para aplicar los cambios, ejecute lo siguiente:

```
service network restart
```

Lo anterior actualizará automáticamente el archivo **/etc/resolv.conf** con el contenido que corresponda.

En **CentOS 5** y **Red Hat™ Enterprise Linux 5** (y versiones anteriores de éstos), edite al archivo **/etc/resolv.conf**:

```
vi /etc/resolv.conf
```

Establezca o confirme los servidores del sistema de resolución de nombres de dominio (DNS). Ejemplo:

```
search dominio.tld
nameserver 8.8.8.8
nameserver 8.8.4.4
```

Si se modifica directamente el archivo **/etc/resolv.conf** los cambios aplican de manera inmediata, sin necesidad de reiniciar el servicio **network**.

35.2.4. Rutas estáticos.

Las rutas estáticas se pueden añadir ejecutando el mandato **ip**, utilizando la siguiente sintaxis:

```
ip route add [red]/[máscara] via [puerta-de-enlace] dev [dispositivo]
```

En el siguiente ejemplo se definirá la ruta estática hacia la red **192.168.3.0** con máscara de 25 bit (**255.255.255.128**), puerta de enlace a través de la dirección IP **172.16.1.36** y a través del dispositivo de red **eth1**:

```
ip route add 192.168.3.0/25 via 172.16.1.36 dev eth1
```

Es un requisito que la puerta de enlace de destino sea alcanzable desde el dispositivo utilizado. Será imposible establecer una ruta estática si es imposible alcanzar la puerta de enlace necesaria. Si sólo se ejecuta el mandato **ip** y se reinicia el servicio **network**, los cambios se perderán.

Si se requiere establecer las rutas estáticas adicionales para obtener conectividad con otras redes y que las configuraciones correspondientes sean permanentes, se pueden generar archivos para cada dispositivo de red que sea necesario, en donde se establecen los valores para puerta de enlace, red a la que se quiere acceder y la máscara de sub-red correspondiente. Los archivos se deben generar dentro del directorio **/etc/sysconfig/network-scripts/** como *route-[dispositivo]* y deben llevar el siguiente formato:

```
GATEWAY0=nnn.nnn.nnn.nnn
ADDRESS0=nnn.nnn.nnn.nnn
NETMASK0=nnn.nnn.nnn.nnn
```

En lugar del parámetro NETMASK, se puede utilizar el parámetro *PREFIX*, definiendo la máscara en formato *CIDR*. Ejemplo:

```
GATEWAY0=nnn.nnn.nnn.nnn
ADDRESS0=nnn.nnn.nnn.nnn
PREFIX0=nn
```

Por citar un ejemplo, imaginemos que nos encontramos dentro de la red 192.168.70.0/25 y se requiere establecer conectividad con las redes 172.16.2.0 y 172.16.3.0, con máscaras 255.255.255.240 (28 bit), a través de las puertas de enlace o enrutadores o encaminadores con direccines IP 192.168.1.2 y 192.168.1.3, correspondientemente para cada red citada, a través del primer dispositivo Ethernet del anfitrión local (eth0).

Genere el archivo **/etc/sysconfig/network-scripts/route-eth0** utilizando un editor de texto:

```
vi /etc/sysconfig/network-scripts/route-eth0
```

La configuración para el escenario descrito arriba, sería la siguiente:

```
GATEWAY0=192.168.1.2
ADDRESS0=172.16.2.0
PREFIX0=28
GATEWAY1=192.168.1.3
ADDRESS1=172.16.3.0
PREFIX1=28
```

Para aplicar los cambios y poder hacer las comprobaciones correspondientes, ejecute lo siguiente:

```
service network restart
```

35.2.5. Función de Reenvío de paquetes para IP versión 4.

Si dispone de al menos 2 dispositivos de red y se tiene planeado implementar un NAT o DNAT, se debe habilitar el reenvío de paquetes para IP versión 4. Esto se realiza editando el archivo **/etc/sysctl.conf** y estableciendo **1** para activar o bien dejar **0** para mantener inactivo:

```
vi /etc/sysctl.conf
```

Y cambiando **net.ipv4.ip_forward = 0** por **net.ipv4.ip_forward = 1**:

```
net.ipv4.ip_forward = 1
```

Para aplicar el cambio, sin reiniciar el sistema, sólo es necesario ejecutar lo siguiente:

```
sysctl -w net.ipv4.ip_forward=1
```

35.2.6. Herramientas para el intérprete de mandatos.

Después de haber configurado todos los parámetros de red deseados, reinicie el servicio **network**, ejecutando lo siguiente:

```
service network restart
```

Para comprobar la conectividad, se puede ejecutar el mandato **ping** hacia cualquier dirección de la red local para tal fin.

```
ping -c3 192.168.70.1
```

La opción **-c3** indica que sólo se harán 3 *pings* hacia la dirección IP de destino.

Para ver la información de todos los dispositivos de red del sistema, se ejecuta lo siguiente:

```
ip addr show
```

En el pasado, lo anterior se hacía utilizando el mandato **ifconfig**.

Para ver la información de un dispositivo de red específico, eth0 en el siguiente ejemplo, se ejecuta lo siguiente:

```
ip addr show eth0
```

En el pasado, lo anterior se hacía utilizando el mandato **ifconfig eth0**.

Para ver la información de estado de todos los dispositivos de red del sistema, se ejecuta lo siguiente:

```
ip link show
```

Para ver la información de estado de de un dispositivos de red en particular, eth0 en el siguiente ejemplo, se ejecuta lo siguiente:

```
ip link show eth0
```

Para detener un dispositivo de red, eth0 en el ejemplo, se ejecuta lo siguiente:

```
ip link set eth0 down
```

En el pasado, lo anterior se hacía utilizando el mandato **ifdown eth0**.

Para iniciar un dispositivo de red, eth0 en el ejemplo, se ejecuta lo siguiente:

```
ip link set eth0 up
```

En el pasado, lo anterior se hacía utilizando el mandato **ifup eth0**.

Para eliminar todos los parámetros de red de un dispositivo específico, eth0 en el ejemplo, se ejecuta lo siguiente.

```
ip addr flush dev eth0
```

Para añadir una dirección IP a un dispositivo, eth0 en el siguiente ejemplo, se ejecuta lo siguiente.

```
ip addr add 192.168.70.61/25 dev eth0
```

Para eliminar una dirección IP a un dispositivo, eth0 en el siguiente ejemplo, se ejecuta lo siguiente.

```
ip addr del 192.168.70.61/25 dev eth0
```

Las rutas estáticas se pueden comprobar utilizando el siguiente mandato:

```
ip route list
```

En el pasado, lo anterior se hacía utilizando el mandato **route**.

Para eliminar todas las rutas estáticas dependientes sólo del dispositivo eth0, se ejecuta lo siguiente:

```
ip route flush dev eth0
```

Para cambiar o establecer la puertas de enlace predeterminada del sistema, 192.168.70.1 en el siguiente ejemplo, a través del dispositivo eth0, se ejecuta lo siguiente:

```
ip route add default via 192.168.70.1 dev eth0
```

Para comprobar si hay resolución de nombres, se puede realizar una consulta hacia los servidores DNS definidos para el sistema, utilizando:

```
host dominio.tld
```

35.2.7. Direcciones IP secundarias

Las direcciones IP secundarias sirven para que el sistema responda para más de una dirección IP a través del mismo dispositivo de red. Son útiles en los casos en los cuales se tiene un servicio de hospedaje de páginas de Internet y se desea que cada sitio tenga su propia dirección IP. También son útiles en los muros cortafuegos donde se quiere que un conjunto de equipos salgan hacia Internet enmascarados con una dirección IP (una LAN, por ejemplo) y otro conjunto de equipos lo hagan con una dirección IP distinta (una DMZ, por ejemplo).

El primer paso es modificar los parámetros **IPADDR** y **NETMASK** de la dirección IP principal, precediendo a éstos el número cero:

```
IPADDR0=192.168.70.101
NETMASK0=255.255.255.128
```

Añada la dirección IP secundaria y la máscara de sub-red con los parámetros **IPADDR1** y **NETMASK1** (o bien **PREFIX1** si prefiere el formato **CIDR**) del siguiente modo:

```
IPADDR0=192.168.70.101
NETMASK0=255.255.255.128
IPADDR1=192.168.70.31
NETMASK1=255.255.255.128
```

Para agregar otra dirección IP secundaria, se añade otro conjunto de parámetros **IPADDR** y **NETMASK**, precedidos con el siguiente número consecutivo:

```
IPADDR0=192.168.70.101
NETMASK0=255.255.255.128
IPADDR1=192.168.70.31
NETMASK1=255.255.255.128
IPADDR2=192.168.70.41
NETMASK2=255.255.255.128
```

Puede utilizar **PREFIX** en lugar de **NETMASK**, definiendo la máscara de sub-red en formato **CIDR**.

```
IPADDR0=192.168.70.101
PREFIX0=25
IPADDR1=192.168.70.31
PREFIX1=25
IPADDR2=192.168.70.41
PREFIX2=25
```

Para aplicar los cambios y poder hacer las comprobaciones correspondientes, ejecute lo siguiente:

```
service network restart
```

La comprobación, al ejecutar el mandato **ip addr show**, deberá regresar algo como lo siguiente

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:23:5a:4b:e8:43 brd ff:ff:ff:ff:ff:ff
    inet 192.168.70.101/25 brd 192.168.70.127 scope global eth0
    inet 192.168.70.31/25 scope global secondary eth0
    inet 192.168.70.41/25 scope global secondary eth0
    inet6 fe80::223:5aff:fe4b:e843/64 scope link
       valid_lft forever preferred_lft forever
```

35.2.8. La función Zeroconf.

De modo predeterminado y a fin de permitir la comunicación entre dos diferentes sistemas a través de un cable RJ45 cruzado (*crossover*), el sistema tiene habilitado **Zeroconf**, también conocido como **Zero Configuration Networking** o **Automatic Private IP Addressing** (APIPA). Es un conjunto de técnicas que automáticamente gestionan la asignación de direcciones IP sin necesidad de configuración de servidores especiales. Permite a usuarios sin conocimientos de redes conectar computadoras, impresoras en red y otros artículos entre sí.

Sin Zeroconf los usuarios sin conocimientos tendrían que configurar servidores especiales como DHCP y DNS para poder establecer conectividad entre dos equipos.

Estando habilitado Zeroconf, se mostrará un registro en la tabla de rutas estáticas para la red **169.254.0.0** al ejecutar el mandato **ip route list**:

```
ip route list
```

Lo anterior devolverá una salida similar a la siguiente:

```
192.168.70.0/25 dev eth0  proto kernel  scope link  src 192.168.70.101
169.254.0.0/16 dev eth0  scope link  metric 1002
default via 192.168.70.1 dev eth0
```

Si se desea desactivar Zeroconf, edite el archivo **/etc/sysconfig/network**:

```
vi /etc/sysconfig/network
```

Añada el parámetro **NOZEROCONF** con el valor **yes**:

```
NETWORKING=yes
HOSTNAME=nombre.dominio.tld
NOZEROCONF=yes
```

Al terminar, reinicie el servicio **network**, a fin de que surtan efecto los cambios:

```
service network restart
```

Para comprobar, ejecute de nuevo con el mandato **ip route list**:

```
ip route list
```

Lo anterior deberá devolver una salida similar a la siguiente, en la cual la ruta para **Zeroconf** ha desaparecido:

```
192.168.70.0/25 dev eth0  proto kernel  scope link  src 192.168.70.101
default via 192.168.70.1 dev eth0
```

Una vez hecho lo anterior, existen dos servicios en el sistema en CentOS y Red Hat™ Enterprise Linux 5 y versiones posteriores, que se pueden desactivar puesto que sirven para establecer la comunicación a través de Zeroconf, estos son **avahi-daemon** y **avahi-dnsconfd**. Desactivar estos dos servicios ahorrará tiempo en el arranque y se consumirán **algunos pocos menos recursos de sistema**.

```
chkconfig avahi-dnsconfd off
chkconfig avahi-daemon off
service avahi-dnsconfd stop
service avahi-daemon stop
```

Muchas aplicaciones y componentes para el modo gráfico dependen de Zeroconf para su correcto funcionamiento. Por tanto, es poco conveniente desactivar este soporte en un sistema de escritorio.

Para más detalles acerca de **Zeroconf**, puede consultarla información disponible en:

- http://www.zeroconf.org/
- http://en.wikipedia.org/wiki/Zeroconf

35.3. Ejercicios.

Este documento coresponde a los ejercicios del documento titulado Configuración de red en GNU/Linux.

35.3.1. Rutas estáticas.

Este ejercicio considera lo siguiente:

1. Se tiene dos equipos de cómputo con GNU/Linux instalado en ambos.

2. **pc1.dominio.tld** tiene una dirección IP 192.168.70.100 con máscara de sub-red 255.255.255.128 en el dispositivo eth0. Una dirección IP 172.16.100.1 con máscara de sub-red 255.255.255.240 en el dispositivo eth1.

3. **pc2.dominio.tld** tiene una dirección IP 192.168.70.102 con máscara de sub-red 255.255.255.128 en el dispositivo eth0. Carece de otros dispositivos de red activos.

Visualice desde **pc2.dominio** los registros de la tabla de rutas estáticas.

```
ip route list
```

Lo anterior devolverá una salida similar a la siguiente:

```
192.168.70.0/25 dev eth0  proto kernel  scope link  src 192.168.70.2  metric 1
default via 192.168.70.1 dev eth0  proto static
```

Intente ejecutar **ping** hacia la dirección recién añadida en **pc1.dominio**.

```
ping -c 3 172.16.100.1
```

El resultado esperado es que **ping** devuelva que hay 100% de pérdida de paquetes.

```
PING 172.16.100.1 (172.16.100.1) 56(84) bytes of data.

--- 172.16.100.1 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 1999ms
```

Proceda a añadir la ruta estática que corresponde especificando la red, mascará de sub-red y puerta de enlace necesarios para llegar hacia 172.16.100.1.

```
ip route add \
172.16.100.0/28 \
via 192.168.70.100 \
dev eth0
```

Visualice de nuevo los registros de la tabla de rutas estáticas.

```
ip route list
```

Lo anterior devolverá una salida similar a la siguiente:

```
172.16.100.0/28 via 192.168.70.100 dev eth0
192.168.70.0/25 dev eth0  proto kernel  scope link  src 192.168.70.2  metric 1
default via 192.168.70.1 dev eth0  proto static
```

Intente ejecutar **ping** hacia la dirección recién añadida en **pc1.dominio**.

```
ping -c 3 172.16.100.1
```

El resultado esperado es que **ping** responda al ping, obteniéndose una salida similar a la siguiente:

```
PING 172.16.100.1 (172.16.100.1) 56(84) bytes of data.
64 bytes from 172.16.100.1: icmp_seq=0 ttl=64 time=0.453 ms
64 bytes from 172.16.100.1: icmp_seq=1 ttl=64 time=0.368 ms
64 bytes from 172.16.100.1: icmp_seq=2 ttl=64 time=0.347 ms

--- 172.16.100.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.347/0.389/0.453/0.048 ms, pipe 2
```

Reinicie el servicio de red, visualice de nuevo los registros de la tabla de rutas estáticas y compruebe que ya no hay respuesta al hacer **ping** hacia 172.16.100.1 porque el registro en la tabla de rutas estáticas fue eliminado al reiniciar el servicio de red.

```
service network restart
ip route list
ping -c 3 172.16.100.1
```

Para hacer permanente el registro en la tabla de rutas estáticas utilice un editor de texto el archivo **/etc/sysconfig/network-scripts/route-eth0** y ponga el siguiente contenido:

```
ADDRESS0=172.16.100.0
NETMASK0=255.255.255.240
GATEWAY0=192.168.70.100
```

Al terminar reinicie el servicio de red.

```
service network restart
```

Visualice nuevamente los registros de la tabla de rutas estáticas.

```
ip route list
```

Lo anterior debe devolver una salida similar a la siguiente:

```
172.16.100.0/28 via 192.168.70.100 dev eth0
192.168.70.0/25 dev eth0  proto kernel  scope link  src 192.168.70.2  metric 1
default via 192.168.70.1 dev eth0  proto static
```

Intente ejecutar **ping** hacia la dirección recién añadida en **pc1.dominio**.

```
ping -c 3 172.16.100.1
```

Reinicie el servicio de red, visualice de nuevo los registros de la tabla de rutas estáticas y compruebe de nuevo que hay respuesta al hacer ping hacia 172.16.100.1.

```
service network restart
route -n
ping -c3 172.16.100.1
```

35.3.2. Ejercicio: Direcciones IP secundarias.

Este ejercicio considera lo siguiente:

1. El dispositivo **eth0** tiene una dirección IP 192.168.70.101/25. Carece de direcciones IP secundarias.

2. Se añadirá como dirección IP secundaria 192.168.70.51/25.

Visualice las interfaces de red activas en el sistema.

```
ip addr show
```

Lo anterior debe devolver una salida similar a la siguiente, donde se mostrará que sólo están activos el dispositivo **eth0** y el correspondiente al dispositivo del retorno del sistema (*loopback*):

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:23:5a:4b:e8:43 brd ff:ff:ff:ff:ff:ff
    inet 192.168.70.101/25 brd 192.168.70.127 scope global eth0
    inet6 fe80::223:5aff:fe4b:e843/64 scope link
       valid_lft forever preferred_lft forever
```

Ejecute el mandato **ping** con la opción **-c3** para comprobar si acaso hay alguna respuesta de la dirección IP secundaria del dispositivo **eth0**.

```
ping -c3 192.168.70.51
```

Lo anterior debe devolver una salida similar a la siguiente:

```
PING 192.168.70.51 (192.168.70.51) 56(84) bytes of data.

--- 192.168.70.51 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 1999ms
```

Ejecute el mandato **ip** del siguiente modo para añadir la dirección IP secundaria 192.168.70.51/25 al dispositivo eth0:

```
ip addr add 192.168.70.51/25 dev eth0
```

Ejecute el mandato **ping** con la opción **-c3** para comprobar que haya respuesta de la dirección IP secundaria del dispositivo **eth0**.

```
ping -c3 192.168.70.51
```

Lo anterior debe devolver una salida similar a la siguiente:

```
PING 192.168.70.51 (192.168.70.51) 56(84) bytes of data.
64 bytes from 192.168.70.51: icmp_seq=0 ttl=64 time=0.453 ms
64 bytes from 192.168.70.51: icmp_seq=1 ttl=64 time=0.368 ms
64 bytes from 192.168.70.51: icmp_seq=2 ttl=64 time=0.347 ms

--- 192.168.70.51 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.347/0.389/0.453/0.048 ms, pipe 2
```

Visualice las interfaces de red activas en el sistema.

```
ip addr show
```

Lo anterior debe devolver una salida similar a la siguiente, donde se mostrará que está activa la dirección IP secundaria del dispositivo **eth0**:

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:23:5a:4b:e8:43 brd ff:ff:ff:ff:ff:ff
    inet 192.168.70.101/25 brd 192.168.70.127 scope global eth0
    inet 192.168.70.51/25 scope global secondary eth0
    inet6 fe80::223:5aff:fe4b:e843/64 scope link
       valid_lft forever preferred_lft forever
```

Reinicie el servicio **network**.

```
service network restart
```

Utilice el mandato **ping** con la opción **-c3** para comprobar si aún hay respuesta desde la dirección IP secundaria del dispositivo **eth0**.

```
ping -c3 192.168.70.51
```

Lo anterior debe devolver una salida similar a la siguiente:

```
PING 192.168.70.51 (192.168.70.51) 56(84) bytes of data.

--- 192.168.70.51 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 1999ms
```

Visualice los dispositivos de red activos en el sistema.

```
ip addr show
```

Lo anterior debe devolver una salida similar a la siguiente, donde se mostrará sólo la dirección IP principal del dispositivo de red **eth0** y la correspondiente al dispositivo del retorno del sistema (*loopback*):

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:23:5a:4b:e8:43 brd ff:ff:ff:ff:ff:ff
    inet 192.168.70.2/25 brd 192.168.70.127 scope global eth0
    inet6 fe80::223:5aff:fe4b:e843/64 scope link
       valid_lft forever preferred_lft forever
```

Para hacer permanente la dirección secundaria en el dispositivo **eth0**, edite el archivo **/etc/sysconfig/network-scripts/ifcfg-eth0** y añada el siguiente contenido **(¡Respete mayúsculas y minúsculas!)**:

```
IPADDR1=192.168.70.51
NETMASK1=255.255.255.128
```

Reinicie el servicio de red.

```
service network restart
```

Visualice las interfaces de red activas en el sistema.

```
ip addr show
```

Lo anterior debe devolver una salida similar a la siguiente, donde nuevamente se mostrará que está activa la dirección IP secundaria del dispositivo **eth0**:

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:23:5a:4b:e8:43 brd ff:ff:ff:ff:ff:ff
    inet 192.168.70.101/25 brd 192.168.70.127 scope global eth0
    inet 192.168.70.51/25 scope global secondary eth0
    inet6 fe80::223:5aff:fe4b:e843/64 scope link
       valid_lft forever preferred_lft forever
```

Utilice el mandato **ping** con la opción **-c3** para comprobar que haya respuesta de la dirección IP secundaria del dispositivo **eth0**:

```
ping -c3 192.168.70.51
```

Lo anterior debe devolver una salida similar a la siguiente:

```
PING 192.168.70.51 (192.168.70.51) 56(84) bytes of data.
64 bytes from 192.168.70.51: icmp_seq=0 ttl=64 time=0.453 ms
64 bytes from 192.168.70.51: icmp_seq=1 ttl=64 time=0.368 ms
64 bytes from 192.168.70.51: icmp_seq=2 ttl=64 time=0.347 ms

--- 192.168.70.51 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.347/0.389/0.453/0.048 ms, pipe 2
```

La dirección IP secundaria del dispositivo **eth0** estará activa la siguiente vez que inicie el sistema operativo.

36. Configuración de VLANs.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales (incluyendo su publicación, a través de cualquier medio, por entidades con fines de lucro). c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en castellano. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

36.1. Introducción.

De acuerdo a Wikipedia, *«una VLAN (acrónimo de **V**irtual **LAN** o Red de Área Local Virtual) es un método para crear redes lógicamente independientes dentro de una misma red física. Varias VLANs pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local, impidiendo que puedan intercambiar datos usando la red local.»*

Su implementación requiere de disponer de conmutadores (switches) con capacidad para VLAN (protocolo 802.1q), los cuales deberán estar **previamente configurados** para gestionar algunas VLANs (y saber cómo hacerlo) y entender perfectamente IP versión 4.

36.2. Equipamiento lógico necesario.

36.2.1. En CentOS, Fedora™ y Red Hat™ Enterprise Linux.

El soporte necesario para configurar VLANs se incluye junto con el paquete **iproute**, el cual se incluye en la instalación predeterminada, pues se trata de un paquete obligatorio e indispensable para el sistema. De manera alternativa puede gestionar también las VLANS a través del paquete **vconfig** (en combinación con el mandato **ifconfig**), ejecutando lo siguiente:

```
yum -y install vconfig
```

36.3. Procedimientos.

Editar el archivo **/etc/sysconfig/network**:

```
vim /etc/sysconfig/network
```

Añadir el siguiente parámetro para activar el soporte para VLAN, mismo que permitirá que posteriormente cargue automáticamente el módulo **8021q** del núcleo de Linux:

```
VLAN=yes
```

Asumiendo que se utiliza la interfaz eth1 para acceder a la red local, editar el archivo de configuración:

```
vim /etc/sysconfig/network-scripts/ifcfg-eth1
```

Quitar todos los parámetros de red que se hayan establecido y dejar el contenido como el del siguiente ejemplo, en el cual se asume que la dirección MAC del dispositivo de red corresponde a **44:87:FC:AA:DD:2D**:

```
DEVICE=eth1
TYPE=Ethernet
BOOTPROTO=none
ONBOOT=yes
HWADDR=44:87:FC:AA:DD:2D
NM_CONTROLED=no
```

Reiniciar el servicio de red a fin de que aplique el cambio y para que cargue de manera automática el módulo **8021q** del núcleo de Linux.

```
service network restart
```

Pueden crearse manera temporal (se perderán luego de reiniciar el sistema) los dispositivos de VLAN del siguiente modo:

```
ip link add link DISPOSITIVO name DISPOSITIVO.ID-VLAN type vlan id ID-VLAN
ip addr add IP/CIDR brd BROADCAST dev DISPOSITIVO.ID-VLAN
ip link set dev DISPOSITIVO.ID-VLAN up
```

Ejemplo:

```
ip link add link eth1 name eth1.2 type vlan id 2
ip addr add 172.16.0.65/26 brd 172.16.0.127 dev eth1.2
ip link set dev eth1.2 up

ip link add link eth1 name eth1.3 type vlan id 3
ip addr add 172.16.0.129/26 brd 172.16.0.191 dev eth1.3
ip link set dev eth1.3 up

ip link add link eth1 name eth1.4 type vlan id 4
ip addr add 172.16.0.193/26 brd 172.16.0.255 dev eth1.4
ip link set dev eth1.4 up
```

De manera alternativa, puede hacer lo mismo utilizando los mandatos **vconfig** y el mandato **ifconfig**, del siguiente modo:

```
vconfig add eth1 2
vconfig add eth1 3
vconfig add eth1 4
ifconfig eth1.2 172.16.0.65 netmask 255.255.255.192
ifconfig eth1.3 172.16.0.129 netmask 255.255.255.192
ifconfig eth1.4 172.16.0.193 netmask 255.255.255.192
```

En caso de que sea necesario, para eliminar los dispositivos de VLAN, puede ejecutar el mandato IP con la siguiente sintaxis:

```
ip link set dev DISPOSITIVO.ID-VLAN down
ip link delete DISPOSITIVO.ID-VLAN
```

Ejemplo:

```
ip link set dev eth1.2 down
ip link delete eth1.2

ip link set dev eth1.3 down
ip link delete eth1.3

ip link set dev eth1.4 down
ip link delete eth1.4
```

De manera alternativa, puede utilizar también el mandato **vconfig** con la opción **rem**, seguido del nombre del dispositivo VLAN. Siguiendo el ejemplo utilizado en este documento, sólo habría que ejecutar lo siguiente:

```
vconfig rem eth1.2
vconfig rem eth1.3
vconfig rem eth1.4
```

Para que los dispositivos de VLANs sean permanentes, es necesario crear, dentro del directorio **/etc/sysconfig/network-scripts**, los archivos de configuración de interfaz, siguiendo el siguiente formato:

```
icfg-DISPOSITIVO.ID-VLAN
```

El número de VLAN, preferentemente debe corresponder son el mimos utilizado en el conmutador principal. Se debe **evitar usar** la VLAN 1 (eth1.1 o eth1.1), 172.16.0.1 como IP para el servidor, así como también evitar utilizar la red 172.16.0.0/**26**, porque suelen corresponder al número de VLAN, dirección IP y segmento de red que regularmente utilizan los conmutadores.

Ejemplo de contenido de **/etc/sysconfig/network-scripts/ifcfg-eth1.2**.

```
DEVICE=eth1.2
TYPE=Ethernet
BOOTPROTO=static
ONBOOT=yes
NM_CONTROLED=no
IPADDR=172.16.0.65
PREFIX=26
BROADCAST=172.16.0.127
NETWORK=172.16.0.64
```

Ejemplo de contenido de **/etc/sysconfig/network-scripts/ifcfg-eth1.3**

```
DEVICE=eth1.3
TYPE=Ethernet
BOOTPROTO=static
ONBOOT=yes
NM_CONTROLED=no
IPADDR=172.16.0.129
PREFIX=26
BROADCAST=172.16.0.191
NETWORK=172.16.0.128
```

Ejemplo de contenido de **/etc/sysconfig/network-scripts/ifcfg-eth1.4**

```
DEVICE=eth1.4
TYPE=Ethernet
BOOTPROTO=static
ONBOOT=yes
NM_CONTROLED=no
IPADDR=172.16.0.193
PREFIX=26
BROADCAST=172.16.0.255
NETWORK=172.16.0.192
```

Reiniciar nuevamente el servicio de red a fin de que inicien las interfaces de VLAN.

```
service network restart
```

Se puede verificar con el mandato **ip** que todas las VLAN estén presentes.

```
ip addr show
```

Lo anterior debe devolver una salida similar a la siguiente:

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
    inet 127.0.0.2/8 brd 127.255.255.255 scope host secondary lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 44:87:FC:AA:DD:2D brd ff:ff:ff:ff:ff:ff
3: eth1.2@eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
    link/ether 44:87:FC:AA:DD:2D brd ff:ff:ff:ff:ff:ff
    inet 172.16.0.65/26 brd 172.16.0.127 scope global eth1.2
    inet6 fe80::a00:27ff:fece:5172/64 scope link
       valid_lft forever preferred_lft forever
4: eth1.3@eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
    link/ether 44:87:FC:AA:DD:2D brd ff:ff:ff:ff:ff:ff
    inet 172.16.0.129/26 brd 172.16.0.191 scope global eth1.3
    inet6 fe80::a00:27ff:fece:5172/64 scope link
       valid_lft forever preferred_lft forever
5: eth1.4@eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
    link/ether 44:87:FC:AA:DD:2D brd ff:ff:ff:ff:ff:ff
    inet 172.16.0.193/26 brd 172.16.0.255 scope global eth1.4
    inet6 fe80::a00:27ff:fece:5172/64 scope link
       valid_lft forever preferred_lft forever
```

De manera alternativa, se puede verificar con el mandato **ifconfig** que todas las VLAN estén presentes.

```
ifconfig
```

La salida debe ser algo similar a lo siguiente:

```
eth1      Link encap:Ethernet  HWaddr 44:87:FC:AA:DD:2D
          inet6 addr: fe80::226:b9ff:fe38:36bc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:13512148 errors:0 dropped:0 overruns:0 frame:0
          TX packets:15358606 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4445028488 (4.1 GiB)  TX bytes:12134964357 (11.3 GiB)
          Interrupt:122 Memory:da000000-da012800

eth1.2    Link encap:Ethernet  HWaddr 44:87:FC:AA:DD:2D
          inet addr:172.16.0.65  Bcast:172.16.0.127  Mask:255.255.255.192
          inet6 addr: fe80::4687:fcff:feaa:dd2d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:4333 (4.2 KiB)

eth1.3    Link encap:Ethernet  HWaddr 44:87:FC:AA:DD:2D
          inet addr:172.16.0.129  Bcast:172.16.0.191  Mask:255.255.255.192
          inet6 addr: fe80::4687:fcff:feaa:dd2d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:4235 (4.1 KiB)

eth1.4    Link encap:Ethernet  HWaddr 44:87:FC:AA:DD:2D
          inet addr:172.16.0.193  Bcast:172.16.0.255  Mask:255.255.255.192
          inet6 addr: fe80::4687:fcff:feaa:dd2d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:3405 (3.3 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:183 errors:0 dropped:0 overruns:0 frame:0
          TX packets:183 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21398 (20.8 KiB)  TX bytes:21398 (20.8 KiB)
```

36.3.1. Administrando direcciones IP de las VLANs a través de un servidor DHCP.

Para alivio de los administradores de sistemas, es posible utilizar el servicio de DHCP para gestionar la administración de direcciones IP a través de un servidor DHCP.

Editar el archivo **/etc/sysconfig/dhcpd** y definir las interfaces de VLAN a utilizar junto con el servidor DHCP.

```
DHCPDARGS="eth1.2 eth1.3 eth1.4";
```

Editar el archivo **/etc/dhcpd.conf** (**CentOS 5** y **Red Hat Enterprise Linux 5**) o bien **/etc/dhcp/dhcpd.conf** (**CentOS 6** y **Red Hat Enterprise Linux 6**), definir una sección por cada red:

```
ddns-update-style interim;
ignore client-updates;
authoritative;
default-lease-time 900;
max-lease-time 7200;
option ip-forwarding off;
option domain-name "red-local.net";
option ntp-servers 200.23.51.205, 132.248.81.29, 148.234.7.30;

shared-network vlan2 {
        subnet 172.16.0.64 netmask 255.255.255.192 {
                option routers 172.16.0.65;
                option subnet-mask 255.255.255.192;
                option broadcast-address 172.16.0.127;
                option domain-name-servers 172.16.0.65;
                option netbios-name-servers 172.16.0.65;
                range 172.16.0.66 172.16.0.126;
        }
}
shared-network vlan3 {
        subnet 172.16.0.128 netmask 255.255.255.192 {
                option routers 172.16.0.129;
                option subnet-mask 255.255.255.192;
                option broadcast-address 172.16.0.191;
                option domain-name-servers 172.16.0.192;
                option netbios-name-servers 172.16.0.192;
                range 172.16.0.130 172.16.0.190;
        }
}
shared-network vlan4 {
        subnet 172.16.0.192 netmask 255.255.255.192 {
                option routers 172.16.0.193;
                option subnet-mask 255.255.255.192;
                option broadcast-address 172.16.0.255;
                option domain-name-servers 172.16.0.193;
                option netbios-name-servers 172.16.0.193;
                range 172.16.0.194 172.16.0.254;
        }
}
```

Reiniciar (o iniciar, según sea el caso) el servicio **dhcpd** y comprobar que funcione correctamente el servicio, conectando algunos equipos a los conmutadores involucrados.

```
service dhcpd restart
```

37. Cómo configurar acoplamiento de tarjetas de red (bonding).

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales (incluyendo su publicación, a través de cualquier medio, por entidades con fines de lucro). c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en castellano. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

37.1. Introducción.

El controlador **bonding**, originalmente creado por **Donald Becker**, está incluido en prácticamente todas las distribuciones de GNU/Linux y permite sumar las capacidades de varias interfaces físicas de red con objeto de crear una interfaz lógica. Esto se lleva a cabo con el objeto de contar con redundancia o bien balanceo de carga.

37.2. Procedimientos.

37.2.1. Archivo de configuración /etc/modprobe.conf.

Se establece el controlador **bonding** para crear la interfaz **bond0** del siguiente modo:

```
alias bonding bond0
```

El controlador puede llevar parámetros que permiten modificar su funcionamiento, de entre los cuales los más importantes son **mode** y **miimon**. A fin de obtener un buen funcionamiento confiable, es importante configurar al menos éstos dos parámetros.

Para fines generales, se puede simplemente configurar del siguiente modo:

```
alias bond0 bonding
options bonding mode=0 miimon=0
```

Lo anterior establece en el parámetro **mode** la política de balanceo de carga y tolerancia a fallos y desactiva en el parámetro **miimon** la supervisión de **MII**, que corresponde la configuración más común.

Al terminar con el archivo **/etc/modprobe.conf**, es importante utilizar el mandato **depmod** para regenerar el archivo **modules.dep** y los archivos mapa de los controladores.

```
depmod
```

Lo anterior solo debe devolver el símbolo de sistemas después de unos segundos.

37.2.1.1. Parámetro mode.

Se utiliza para establecer la política baja la cual se hará trabajar las tarjetas en conjunto. Los posibles valores son:

0 (cero): Establece una política de **Round-Robin**, que es un algoritmo que asigna una carga equitativa y ordenada a cada proceso, para proporcionar **tolerancia a fallos** y **balanceo de carga** entre los miembros del arreglo de dispositivos. Todas las transmisiones de datos son enviadas y recibidas de forma secuencial en cada interfaz esclava del arreglo empezando con la primera que esté disponible. **Es la política predeterminada** del controlador y la que funciona para la mayoría de los casos.

1 (uno): Establece una política de respaldo activo que proporciona **tolerancia a fallos**. Todo el tráfico se transmite a través de una tarjeta y solo se utilizará la otra en caso de que falle la primera.

2 (dos): Establece una política **XOR** (*exclusive-or*, exclusiva-o) para proporcionar **tolerancia a fallos** y **balanceo de carga**. Este algoritmo compara las solicitudes entrantes de las direcciones **MAC** hasta que coinciden para la dirección **MAC** (**M**edia **A**ccess **C**ontrol) de una de las tarjetas esclavas. Una vez que se establece el enlace, las transmisiones de datos de datos son enviadas en forma secuencial empezando con la primera interfaz disponible.

3 (tres): Establece una política de **Round-Robin**, para proporcionar **tolerancia a fallos** y **balanceo de carga**. Todas las transmisiones de datos son enviadas de forma secuencial en cada interfaz esclava del arreglo empezando con la primera que esté disponible.

En el siguiente ejemplo se establece la política 0 (cero):

```
options bonding mode=0
```

37.2.1.2. Parámetro miimon.

Se utiliza para especificar cada cuantos milisegundos se debe supervisar el enlace **MII** (**M**edia **I**ndependent **I**nterface). Se utiliza cuando se necesita alta disponibilidad para verificar si la interfaz está activa y verificar si hay un cable de red conectado. En el siguiente ejemplo se establecen 100 milisegundos:

```
options bonding mode=0 miimon=100
```

Se requiere que **todos** los controladores del arreglo de tarjetas tengan soporte para **MII**. Para verificar si el controlador de la tarjeta tiene soporte para **MII**, se utiliza el mandato **ethtool**, donde la salida debe devolver el parámetro **Link Detected** con el valor **yes**. Ejemplo:

```
ethtool eth0
```

Lo anterior debe devolver algo similar a lo siguiente:

```
Settings for eth0:
        Supported ports: [ TP MII ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
        Supports auto-negotiation: Yes
        Advertised link modes:  10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
        Advertised auto-negotiation: Yes
        Speed: 100Mb/s
        Duplex: Half
        Port: MII
        PHYAD: 32
```

```
        Transceiver: internal
        Auto-negotiation: on
        Supports Wake-on: pumbg
        Wake-on: d
        Current message level: 0x00000007 (7)
        Link detected: yes
```

Para desactivar esta función, se utiliza el valor 0 (cero). Ejemplo:

```
options bonding mode=0 miimon=0
```

37.2.2. Archivo de configuración /etc/sysconfig/network-scripts/bond0.

Este se configura con los mismo parámetros que una tarjeta normal. Requiere los parámetros **ONBOOT**, **BOOTPROTO**, **DEVICE**, **IPADDR**, **NETMASK** y **GATEWAY**.

En el siguiente ejemplo se configura la interfaz **bond0** con la dirección IP estática 192.168.0.1, máscara de subred 255.255.255.0, puerta de enlace 192.168.0.254 y la interfaz inicia junto con el sistema creando el archivo **/etc/sysconfig/network-scripts/ifcfg-bond0** con el siguiente contenido:

```
DEVICE=bond0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192-168.0.1
NETMASK=255.255.255.0
GATEWAY=192.168.0.254
```

Las interfaces de red a utilizar como esclavas se configuran de la siguiente forma, considerando que se tiene eth0 y eth1, el contenido del archivo **/etc/sysconfig/network-scripts/ifcfg-eth0** sería:

```
DEVICE=eth0
BOOTPROTO=none
ONBOOT=no
SLAVE=yes
MASTER=bond0
```

Y el contenido del archivo **/etc/sysconfig/network-scripts/ifcfg-eth1** sería:

```
DEVICE=eth1
BOOTPROTO=none
ONBOOT=no
SLAVE=yes
MASTER=bond0
```

37.2.3. Iniciar, detener y reiniciar el servicio network.

Para ejecutar por primera vez el servicio **network** tras configurar el acoplamiento de tarjetas, utilice:

```
service network start
```

Para hacer que los cambios hechos tras modificar la configuración surtan efecto, utilice:

```
service network restart
```

Para detener el servicio **network** utilice:

```
service network stop
```

37.3. Comprobaciones.

Para verificar que la interfaz lógica quedó configurada, en el caso de haber utilizado las interfaces eth0 y eth1, utilice:

```
ifconfig
```

Lo anterior debe devolver algo similar a lo siguiente:

```
bond0     Link encap:Ethernet  HWaddr 00:01:80:41:9C:8A
          inet addr:192.168.1.64  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::201:80ff:fe41:9c8a/64 Scope:Link
          UP BROADCAST RUNNING MASTER MULTICAST  MTU:1500  Metric:1
          RX packets:5128 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3817 errors:7 dropped:0 overruns:0 carrier:0
          collisions:3 txqueuelen:0
          RX bytes:3493139 (3.3 MiB)  TX bytes:495025 (483.4 KiB)

eth0      Link encap:Ethernet  HWaddr 00:01:80:41:9C:8A
          inet6 addr: fe80::201:80ff:fe41:9c8a/64 Scope:Link
          UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
          RX packets:5056 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3781 errors:0 dropped:0 overruns:0 carrier:0
          collisions:3 txqueuelen:1000
          RX bytes:3474685 (3.3 MiB)  TX bytes:488632 (477.1 KiB)
          Interrupt:11 Base address:0xc000

eth1      Link encap:Ethernet  HWaddr 00:01:80:41:9C:8A
          inet6 addr: fe80::201:80ff:fe41:9c8a/64 Scope:Link
          UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
          RX packets:72 errors:0 dropped:0 overruns:0 frame:0
          TX packets:36 errors:7 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:18454 (18.0 KiB)  TX bytes:6393 (6.2 KiB)
          Interrupt:10

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:6138 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6138 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:8364864 (7.9 MiB)  TX bytes:8364864 (7.9 MiB)
```

Para verificar que las interfaces de red están funcionando correctamente y que hay un cable de red conectado a éstas, se utiliza el mandato **ethtool** del siguiente modo:

```
ethtool eth0 |grep "Link detected"
ethtool eth1 |grep "Link detected"
```

Si ambas tarjetas tiene soporte para **MII**, lo anterior debe devolver lo siguiente:

```
        Link detected: yes
        Link detected: yes
```

37.4. Bibliografía.

- Thomas Davis: http://www.linuxfoundation.org/en/Net:Bonding

- Thomas Davis: http://www.kernel.org/pub/linux/kernel/people/marcelo/linux-2.4/Documentation/networking/bonding.txt

38. Conexión a redes inalámbricas (Wifi) desde terminal.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales (incluyendo su publicación, a través de cualquier medio, por entidades con fines de lucro). c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en castellano. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

38.1. Introducción.

Configurar y conectarse a una red Wifi desde la interfaz gráfica es un procedimiento relativamente trivial, dejando que todos los procedimientos los realicen NetworkManager o Connman. Sin embargo ha circunstancias en las cuales puede ser necesario conectarse a una red Wifi desde una terminal. A continuación describiré los procedimientos para conectarse a los dos tipos de redes Wifi más utilizados, WEP y WPA, con configuraciones básicas utilizadas en dispositivos como serían los puntos de acceso de los modem ADSL de Prodigy Infinitum.

38.1.1. ¿Que es WPA? ¿Por qué debería usarlo en lugar de WEP?

WPA (**W**i-Fi **P**rotected **A**ccess) y **WPA2** es una clase de sistemas para el aseguramiento de redes inalámbricas. **WPA** fue creado en respuesta a las serias debilidades de otros protocolos como **WEP** (**W**ired **E**quivalent **P**rivacy). Implementa la mayoría de lo que conforma el estándar **IEEE 802.11i** y fue diseñado para funcionar con todas los dispositivos para redes inalámbricas, excepto los puntos de acceso de primera generación. **WPA2** implementa todo el estándar **IEEE 802.11i**, pero no funciona con muchos dispositivos viejos.

WPA fue creado por el grupo industrial y comercial Alianza Wi-Fi, dueños de la marca registrada **Wi-Fi** y certificadores de los dispositivos que ostenten dicho nombre.

Los datos utilizan el algoritmo RC4 con una clave de 128 bits y un vector de inicialización de 48 bits. Una de las mejoras más sobresalientes sobre su predecesor, **WEP**, es **TKIP** (**T**emporal **K**ey **I**ntegrity **P**rotocol o Protocolo de integridad de clave temporal), el cual consiste en el cambio dinámico mientras se utiliza el sistema. Cuando se combina con **Vectores de Inicialización** mayores, hace considerablemente más difícil realizar ataques para la obtención de llaves, como ocurre con **WEP**.

Además de proporcionar autenticación y ciframiento, **WPA** proporciona mejor integridad de la carga útil. La verificación de redundancia cíclica (**CRC** o **C**yclic **R**edundancy **C**heck) utilizada en **WEP** es insegura porque permite alterar la carga útil y actualizar el mensaje de verificación de redundancia cíclica sin necesidad de conocer la clave **WEP**. En cambio **WPA** utiliza un **Código de Integridad de Mensaje** (**MIC** o **M**essage **I**ntegrity **C**ode) que es en realidad un algoritmo denominado *«Michael»*, que fue el más fuerte que se pudo utilizar con dispositivos antiguos para redes inalámbricas a fin de no dejar obsoletos a éstos. El **Código de Integridad de Mensaje** de **WPA** incluye un un mecanismo que contrarresta los intentos de ataque para vulnerar **TKIP** y bloques temporales.

En resumen, **WPA** hace más difícil vulnerar las redes inalámbricas al incrementar los tamaños de las claves y **Vectores de Inicialización**, reduciendo el número de paquetes enviados con claves relacionadas y añadiendo un sistema de verificación de mensajes.

Además de poder utilizar una clave compartida (**PSK** o **P**re-**S**hared **K**ey), lo cual suple la complejidad de implementación de un servidor de autenticación **802.1X** en hogares y oficinas pequeñas, **WPA** puede utilizar **Protocolos Extensibles de Autenticación** (**EAP** o (**E**xtensible **A**uthentication **P**rotocol), como los siguientes:

- EAP-TLS
- EAP-TTLS/MSCHAPv2
- PEAPv0/EAP-MSCHAPv2
- PEAPv1/EAP-GTC
- EAP-SIM
- EAP-LEAP

Entre los diversos servidores que pueden utilizarse para este tipo de implementaciones, está **FreeRADIUS**. **Alcance Libre** cuenta con un modesto documento para la configuración de esta implementación.

38.2. Equipamiento lógico necesario.

38.2.1. Instalación a través de yum.

Se requieren los paquetes **wireless-tools** y **wpa_supplicant**. Para instalar o actualizar el equipamiento lógico necesario en **CentOS**, **Fedora** o **Red Hat™ Enterprise Linux** y versiones posteriores de éstos, sólo se necesita ejecutar como **root** lo siguiente:

```
yum -y install wireless-tools wpa_supplicant
```

Si utiliza **openSUSE** o **SUSE Linux Enterprise**, sólo se necesita ejecutar lo siguiente para instalar o actualizar el equipamiento lógico necesario, en caso de que éste estuviese ausente:

```
yast -i wireless-tools wpa_supplicant
```

Si utiliza **Debian** o **Ubuntu** y versiones posteriores, sólo se necesita ejecutar lo siguiente para instalar o actualizar el equipamiento lógico necesario, en caso de que éste estuviese ausente:

```
sudo apt-get install wireless-tools wpa_supplicant
```

38.2.2. Preparativos.

En sistemas operativos basados sobre **CentOS**, **Fedora**, **Red Hat Enterprise Linux**, **openSUSE** y **SUSE Linux Enterprise**, el primer paso consiste en cambiarse al usuario **root**:

```
su -l
```

En sistemas operativos basados sobre Ubuntu Linux, se puede utilizar el mandato **sudo** para todos los procedimientos, precediendo todos los mandatos utilizados con **sudo**.

```
sudo cualquier mandato utilizado
```

Ejemplos:

```
sudo ifup lo
sudo iwconfig wlan0
sudo iwlist wlan0 scan
```

Debido a que seguramente el servicio **NetworkManager** hará conflicto con los procedimientos, se debe detener éste:

```
service NetworkMananger stop
```

Muchos componentes del sistema requieren que esté activa la interfaz de retorno del sistema (loopback), por lo que es importante iniciar ésta:

```
ifup lo
```

Para poder comenzar a utilizar la interfaz Wifi, solo basta ejecutar el mandato **iwconfig** sobre dicha interfaz:

```
iwconfig wlan0
```

Es buena idea realizar un escaneado de las redes Wifi disponibles para asegurarse se puede acceder a la red Wifi deseada y para determinar el protocolo a utilizar:

```
iwlist wlan0 scan
```

38.2.3. Autenticando en el punto de acceso.

38.2.3.1. A través de redes WEP.

Para redes inalámbricas con autenticación a través de cifrado WEP, que se caracterizan por tener una seguridad muy pobre, el procedimiento es simple. Sólo basta utilizar dos mandatos. El primero define el nombre del punto de acceso a utilizar:

```
iwconfig wlan0 essid punto-de-acceso
```

El segundo mandato se utiliza para definir la clave de acceso a utilizar, sea de 64 o 128 bit.

```
iwconfig wlan0 key clave-de-acceso
```

Si se utiliza una clave WEP tipo ASCII, se define de la siguiente manera:

```
iwconfig wlan0 key s:clave-de-acceso
```

38.2.3.2. A través de redes WPA.

Se procede a determinar el nombre de la red Wifi a utilizar y la clave de acceso. El mandato **wpa_passphrase** se utilizará para generar un archivo de configuración a utilizar posteriormente:

```
wpa_passphrase punto-de-acceso clave-de-acceso > /root/wpa.conf
```

Si se realiza el procedimiento desde Ubuntu Linux, el mandato anterior fallará si se utiliza **sudo** debido a limitaciones de seguridad de **sudo** y deberá utilizarse entonces el siguiente:

```
sudo bash -c "wpa_passphrase punto-de-acceso clave-de-acceso > /root/wpa.conf"
```

Lo anterior generará el archivo **wpa.conf** dentro del directorio de inicio del usuario root.

Para iniciar la autenticación con la red Wifi, se utiliza el mandato **wpa_supplicant** con las opciones **-B**, para enviar el procesos a segundo plano, -D, para especificar el controlador a utilizar y -c, para especificar el archivo de configuración creado en el paso anterior.

```
wpa_supplicant -B -Dwext -iwlan0 -c/root/wpa.conf
```

38.2.4. Asignando parámetros de red a la interfaz.

38.2.4.1. Utilizando dhclient.

Lo más común es utilizar el mandato **dhclient** para dejar que el servidor DHCP del punto de acceso o la LAN se encargue de asignar los parámetros de red para la interfaz. Es buena idea indicar a **dhclient** que libere el préstamo que estuviera asignado en el servidor DHCP:

```
dhclient -r
```

Para obtener una nueva dirección IP, se utiliza el mandato **dhclient** de la siguiente manera:

```
dhclient wlan0
```

38.2.4.2. Asignando manualmente los parámetros de red.

Si se conocen los datos para la configuración de red, también es posible asignarlos manualmente. En el siguiente ejemplo, se asigna a la interfaz wlan0 la dirección IP 192.168.70.50, con máscara de subred 255.255.255.128 (25 bit) y puerta de enlace 192.168.70.1:

```
ip addr add 192.168.70.50/25 dev wlan0
ip route add default via 192.168.70.1 dev wlan0
```

Para definir el servidor DNS, como el usuario **root**, se edita el archivo **/etc/resolv.conf** y se define la dirección IP del servidor DNS a utilizar. En el siguiente ejemplo, se define 192.168.70.1 como servidor DNS:

```
echo "nameserver 192.168.70.1" > /etc/resolv.conf
```

Si se realiza el procedimiento desde Ubuntu Linux o Debian, el mandato anterior fallará si se utiliza **sudo** debido a limitaciones de seguridad de **sudo** y deberá utilizarse entonces el siguiente:

```
sudo bash -c "echo 'nameserver 192.168.70.1' > /etc/resolv.conf"
```

38.2.4.3. Asignación permanente de parámetros de red en CentOS, Fedora y Red Hat Enterprise Linux.

Solo es necesario crear el archivo de interfaz, dentro de **/etc/sysconfig/network-scripts/** siguiendo el siguiente formato:

```
ifcfg-Auto_punto-de-acceso
```

Como ejemplo, si se desea conectar el sistema a un punto de acceso denominado **alcance2**, se debe crear el archivo **/etc/sysconfig/network-scripts/ifcfg-Auto_alcance2**:

```
vim /etc/sysconfig/network-scripts/ifcfg-Auto_alcance2
```

Si se va a conectar a través de DHCP y utilizar cifrado **WEP**, poner el siguiente contenido:

```
NAME="Auto alcance2"
ONBOOT=yes
TYPE=Wireless
BOOTPROTO=dhcp
ESSID=alcance2
MODE=Managed
SECURITY_MODE=open
DEFAULTKEY=1
PEERDNS=yes
PEERROUTES=yes
DHCP_CLIENT_ID=nombre-equipo
DHCP_HOSTNAME=nombre-equipo
```

Si se va a conectar a través de DHCP y utilizar cifrado **WPA**, poner el siguiente contenido:

```
NAME="Auto alcance2"
ONBOOT=yes
TYPE=Wireless
BOOTPROTO=dhcp
ESSID=alcance2
MODE=Managed
KEY_MGMT=WPA-PSK
PEERDNS=yes
PEERROUTES=yes
DHCP_CLIENT_ID=nombre-equipo
DHCP_HOSTNAME=nombre-equipo
```

Para la clave de acceso del punto de acceso, es necesario crear el archivo **/etc/sysconfig/network-scripts/keys-Auto_alcance2**:

```
vim /etc/sysconfig/network-scripts/keys-Auto_alcance2
```

Si se va a conectar por WEP, poner el siguiente contenido:

```
KEY_PASSPHRASE1=clave-de-acceso
```

Si se va a conectar por WPA, poner el siguiente contenido:

```
WPA_PSK=clave-de-acceso
```

Hecho todo lo anterior, será posible iniciar la interfaz ejecutando el siguiente mandato:

```
ip link set wlan0 up
```

Cuando sea necesario detener la interfaz, se ejecuta el siguiente mandato.

```
ip link set wlan0 down
```

38.3. Bibliografía.

- http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access
- http://www.alcancelibre.org/article.php/20070404112747533
- http://www.alcancelibre.org/article.php/20070403184255131

39. Uso del mandato nc (Netcat).

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales (incluyendo su publicación, a través de cualquier medio, por entidades con fines de lucro). c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en castellano. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

39.1. Introducción.

39.1.1. Acerca de Netcat.

El mandato **netcat** o **nc** es una herramienta utilizada para supervisar y escribir sobre conexiones tanto **TCP** como **UDP**. Puede abrir conexiones **TCP**, enviar paquetes **UDP**, escuchar peticiones sobre puertos arbitrarios tanto **TCP** como **UDP**, permite supervisar puertos abiertos y otras muchas cosas más, tanto para **IPv4** como **IPv6**. Es una de las herramientas de diagnóstico y seguridad más populares y también una de las más valoradas por la comunidad de usuarios de GNU/Linux.

39.2. Equipamiento lógico necesario.

39.2.1. En CentOS, Fedora™ y Red Hat™ Enterprise Linux.

Para instalar **Netcat**, ejecute lo siguiente:

```
yum -y install nc
```

39.2.2. En openSUSE™ y SUSE™ Linux Enterprise.

Para instalar **Netcat**, ejecute lo siguiente:

```
yast -i netcat
```

39.3. Procedimientos en CentOS, Fedora™ y Red Hat™ Enterprise Linux.

El manual completo del mandato **nc** puede consultarse ejecutando lo siguiente:

```
man 1 nc
```

39.3.1. Conexiones simples.

Para iniciar una conexión hacia algún puerto en algún sistema, se utiliza el mandato **nc** seguido de una dirección **IP** y un puerto al cual conectarse. En el siguiente ejemplo se realizará una conexión hacia el puerto 25 (**SMTP**) de **127.0.0.1**:

```
nc 127.0.0.1 25
```

Si hay un servidor de correo funcionado, lo anterior puede devolver una salida similar a la siguiente, donde requerirá escribir *quit* y pulsar la tecla ENTER para cerrar la conexión:

```
220 localhost.localdomain ESMTP ; Wed, 28 May 2008 10:24:52 -0500
quit
221 2.0.0 localhost.localdomain closing connection
```

39.3.2. Revisión de puertos.

Para revisar los puertos abiertos, se utiliza el mandato **nc** con la opción , **-z** para solicitar se trate de escuchar por puertos abiertos y un puerto o rango de puertos. En el siguiente ejemplo, se pide al mandato **nc** revisar cuáles puertos **TCP** (modo predeterminado) están abiertos dentro del rango que va del puerto 21 al puerto 25.

```
nc -vz 127.0.0.1 21-25
```

Lo anterior puede devolver una salida similar a la siguiente, si se encontrasen abiertos los puertos 21, 22 y 25.

```
Connection to 127.0.0.1 21 port [tcp/ftp] succeeded!
Connection to 127.0.0.1 22 port [tcp/ssh] succeeded!
Connection to 127.0.0.1 25 port [tcp/smtp] succeeded!
```

De manera opcional, se pueden revisar si están abiertos los puertos UDP abiertos añadiendo la opción **-u**. En el siguiente ejemplo se solicita al mandato **nc** revisar cuáles puertos **UDP** se encuentran abiertos entre el rango comprendido entre los puertos 21 al 80.

```
nc -zu 127.0.0.1 21-80
```

Lo anterior puede devolver una salida similar a la siguiente, donde se asume que se encuentran abiertos los puertos **UDP** 53, 67 y 68:

```
Connection to 127.0.0.1 53 port [udp/domain] succeeded!
Connection to 127.0.0.1 67 port [udp/bootps] succeeded!
Connection to 127.0.0.1 68 port [udp/bootpc] succeeded!
```

Si se quiere obtener una salida más descriptiva, sólo es necesario ejecutar el mandato **nc** con las opciones **-vz** y la dirección **IP** si se quiere revisar puertos **TCP** abiertos o bien **nc -vzu** para puertos **UDP** abiertos, donde la opción **-v** define se devuelva una salida **más descriptiva**. En el siguiente ejemplo se pide al mandato **nc** revisar los puertos **TCP** abiertos entre el puerto 20 al 25.

```
nc -vz 127.0.0.1 20-25
```

La salida de lo anterior también devolverá, a diferencia de utilizar sólo la opción **-z**, cuáles puertos están cerrados en el rango especificado.

```
nc: connect to 127.0.0.1 port 20 (tcp) failed: Connection refused
Connection to 127.0.0.1 21 port [tcp/ftp] succeeded!
Connection to 127.0.0.1 22 port [tcp/ssh] succeeded!
nc: connect to 127.0.0.1 port 23 (tcp) failed: Connection refused
nc: connect to 127.0.0.1 port 24 (tcp) failed: Connection refused
Connection to 127.0.0.1 25 port [tcp/smtp] succeeded!
```

39.3.3. Creando un modelo cliente servidor.

Es relativamente simple crear un modelo cliente/servidor. Desde una terminal que será utilizada para iniciar un modelo de servidor, se utiliza el mandato **nc** con la opción **-l** (listen o escuchar) seguida de un número de puerto que esté desocupado. Esto hará que nc se comporte como servidor escuchando peticiones en un puerto arbitrario. En el siguiente ejemplo se hará que mandato **nc** funcione como servidor escuchando peticiones en el puerto **22222**.

```
nc -l 22222
```

Para establecer la conexión como cliente, desde otra terminal se inicia el mandato **nc** especificando como argumentos una dirección IP y el numero de puerto al que se quiera conectar. En el siguiente ejemplo se realiza la conexión al puerto **22222** de **127.0.0.1** (anfitrión local):

```
nc 127.0.0.1 22222
```

Con lo anterior, todo lo que se escriba desde la terminal como cliente podrá ser visto en la terminal como servidor.

39.3.4. Transferencia de datos.

Tomando el ejemplo anterior, es posible realizar transferencia de datos desde una terminal como cliente hacia una terminal como servidor. La única diferencia es que en el servidor se cambia el direccionamiento de la salida estándar (**STDOUT**) de la terminal, hacia un archivo, como se ejemplifica a continuación:

```
nc -l 22222 > algo.out
```

En el cliente se realiza algo similar. En lugar de ingresar datos desde la conexión. Se hace a partir de un archivo con contenido de la siguiente forma:

```
nc 127.0.0.1 22222 < algo.in
```

En el ejemplo descrito se realiza la transferencia de datos del archivo **algo.in**, desde el proceso como cliente, hacia el archivo **algo.out**, en el proceso como servidor.

39.4. Procedimientos en openSUSE™ y SUSE™ Linux Enterprise.

El manual completo del mandato **netcat** puede consultarse ejecutando lo siguiente:

```
man 1 netcat
```

39.4.1. Conexiones simples.

Para iniciar una conexión hacia algún puerto en algún sistema, se utiliza el mandato **netcat** seguido de una dirección **IP** y un puerto al cual conectarse. En el siguiente ejemplo se realizará una conexión hacia el puerto 25 (**SMTP**) de **127.0.0.1**:

```
netcat 127.0.0.1 25
```

Si hay un servidor de correo funcionado, lo anterior puede devolver una salida similar a la siguiente, donde requerirá escribir *quit* y pulsar la tecla ENTER para cerrar la conexión:

```
220 localhost.localdomain ESMTP ; Wed, 28 May 2008 10:24:52 -0500
quit
221 2.0.0 localhost.localdomain closing connection
```

39.4.2. Revisión de puertos.

Para revisar los puertos abiertos, se utiliza el mandato **netcat** con la opción , **-z** para solicitar se trate de escuchar por puertos abiertos y un puerto o rango de puertos. En el siguiente ejemplo, se pide al mandato **netcat** revisar cuáles puertos **TCP** (modo predeterminado) están abiertos dentro del rango que va del puerto 21 al puerto 25.

```
netcat -vz 127.0.0.1 21-25
```

Lo anterior puede devolver una salida similar a la siguiente, si se encontrasen abiertos los puertos 21, 22 y 25.

```
Connection to 127.0.0.1 21 port [tcp/ftp] succeeded!
Connection to 127.0.0.1 22 port [tcp/ssh] succeeded!
Connection to 127.0.0.1 25 port [tcp/smtp] succeeded!
```

De manera opcional, se pueden revisar si están abiertos los puertos UDP abiertos añadiendo la opción **-u**. En el siguiente ejemplo se solicita al mandato **netcat** revisar cuáles puertos **UDP** se encuentran abiertos entre el rango comprendido entre los puertos 21 al 80.

```
netcat -zu 127.0.0.1 21-80
```

Lo anterior puede devolver una salida similar a la siguiente, donde se asume que se encuentran abiertos los puertos **UDP** 53, 67 y 68:

```
Connection to 127.0.0.1 53 port [udp/domain] succeeded!
Connection to 127.0.0.1 67 port [udp/bootps] succeeded!
Connection to 127.0.0.1 68 port [udp/bootpc] succeeded!
```

Si se quiere obtener una salida más descriptiva, sólo es necesario ejecutar el mandato **netcat** con las opciones **-vz** y la dirección **IP** si se quiere revisar puertos **TCP** abiertos o bien **netcat -vzu** para puertos **UDP** abiertos, donde la opción **-v** define se devuelva una salida **más descriptiva**. En el siguiente ejemplo se pide al mandato **netcat** revisar los puertos **TCP** abiertos entre el puerto 20 al 25.

```
netcat -vz 127.0.0.1 20-25
```

La salida de lo anterior también devolverá, a diferencia de utilizar sólo la opción **-z**, cuáles puertos están cerrados en el rango especificado.

```
netcat: connect to 127.0.0.1 port 20 (tcp) failed: Connection refused
Connection to 127.0.0.1 21 port [tcp/ftp] succeeded!
Connection to 127.0.0.1 22 port [tcp/ssh] succeeded!
netcat: connect to 127.0.0.1 port 23 (tcp) failed: Connection refused
netcat: connect to 127.0.0.1 port 24 (tcp) failed: Connection refused
Connection to 127.0.0.1 25 port [tcp/smtp] succeeded!
```

39.4.3. Creando un modelo cliente servidor.

Es relativamente simple crear un modelo cliente/servidor. Desde una terminal que será utilizada para iniciar un modelo de servidor, se utiliza el mandato **netcat** con la opción **-l** (listen o escuchar) seguida de un número de puerto que esté desocupado. Esto hará que netcat se comporte como servidor escuchando peticiones en un puerto arbitrario. En el siguiente ejemplo se hará que mandato **netcat** funcione como servidor escuchando peticiones en el puerto **22222**.

```
netcat -l 22222
```

Para establecer la conexión como cliente, desde otra terminal se inicia el mandato **netcat** especificando como argumentos una dirección IP y el numero de puerto al que se quiera conectar. En el siguiente ejemplo se realiza la conexión al puerto **22222** de **127.0.0.1** (anfitrión local):

```
netcat 127.0.0.1 22222
```

Con lo anterior, todo lo que se escriba desde la terminal como cliente podrá ser visto en la terminal como servidor.

39.4.4. Transferencia de datos.

Tomando el ejemplo anterior, es posible realizar transferencia de datos desde una terminal como cliente hacia una terminal como servidor. La única diferencia es que en el servidor se cambia el direccionamiento de la salida estándar (**STDOUT**) de la terminal, hacia un archivo, como se ejemplifica a continuación:

```
netcat -l 22222 > algo.out
```

En el cliente se realiza algo similar. En lugar de ingresar datos desde la conexión. Se hace a partir de un archivo con contenido de la siguiente forma:

```
netcat 127.0.0.1 22222 < algo.in
```

En el ejemplo descrito se realiza la transferencia de datos del archivo **algo.in**, desde el proceso como cliente, hacia el archivo **algo.out**, en el proceso como servidor.

40. Como utilizar Netstat.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales (incluyendo su publicación, a través de cualquier medio, por entidades con fines de lucro). c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en castellano. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

40.1. Introducción.

40.1.1. Acerca de Netstat

Netstat es una herramienta utilizada para supervisar las conexiones de red, tablas de encaminamiento, estadísticas de interfaces y asignaturas de multidifusión. Se utiliza principalmente para encontrar problemas en una red y para medir el tráfico de red como una forma de calcular el desempeño de ésta.

40.2. Procedimientos.

Para visualizar todas las conexiones activas en el sistema, tanto TCP como UDP, se utiliza la opción -a.

```
netstat -a
```

Debido a que la cantidad de datos puede ser mucha para ser visualizada con comodidad en la pantalla del monitor, se puede utilizar el mandato less como subrutina.

```
netstat -a | less
```

A continuación se muestra un ejemplo de la salida:

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 *:netbios-ssn               *:*                         LISTEN
tcp        0      0 *:submission                *:*                         LISTEN
tcp        0      0 *:sunrpc                    *:*                         LISTEN
tcp        0      0 *:x11                       *:*                         LISTEN
tcp        0      0 *:5904                      *:*                         LISTEN
tcp        0      0 *:webcache                  *:*                         LISTEN
udp        0      0 *:filenet-tms               *:*
udp        0      0 *:filenet-nch               *:*
udp        0      0 *:filenet-rmi               *:*
udp        0      0 *:filenet-pa                *:*
udp        0      0 192.168.122.1:netbios-ns    *:*
udp        0      0 servidor00.c:netbios-ns     *:*
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node Path
unix  2      [ ACC ]     STREAM     LISTENING     17530  @/tmp/fam-root-
unix  2      [ ACC ]     STREAM     LISTENING     7944   /dev/gpmctl
unix  2      [ ACC ]     STREAM     LISTENING     6991   /var/run/audit_events
unix  2      [ ACC ]     STREAM     LISTENING     7409   /var/run/dbus/system_bus_socket
unix  2      [ ACC ]     STREAM     LISTENING     7506   /var/run/pcscd.comm
unix  2      [ ACC ]     STREAM     LISTENING     7647   /var/run/acpid.socket
unix  2      [ ACC ]     STREAM     LISTENING     7737   /var/run/cups/cups.sock
unix  2      [ ACC ]     STREAM     LISTENING     16795  @/tmp/dbus-4Uato6eJUH
```

Para mostrar solo las conexiones activas por TCP, se utiliza:

```
netstat -t
```

Para mostrar solo las conexiones activas por UDP, se utiliza:

```
netstat -u
```

Para mostrar las estadísticas de uso para todos los tipos de conexiones, se utiliza:

```
netstat -s
```

Lo anterior puede devolver una salida similar a la siguiente:

```
Ip:x  2      [ ]         DGRAM                    8015
    8005 total packets received                   7929
    2 with invalid addressesAM                    7896
    0 forwarded]         DGRAM                    7866
    0 incoming packets discarded                  7505
    7928 incoming packets delivered CONNECTED     7412
    7905 requests sent outTREAM     CONNECTED     7411
Icmp: 3      [ ]         STREAM     CONNECTED     7349
    19 ICMP messages receivedAM     CONNECTED     7348
    0 input ICMP message failed.                  7199
    ICMP input histogram:DGRAM                    7071
        destination unreachable: 18               6947
        echo requests: 1 DGRAM                    6917
    19 ICMP messages sentSTREAM     CONNECTED     6845
    0 ICMP messages failedTREAM     CONNECTED     6844
    ICMP output histogram:a | less
        destination unreachable: 18
        echo replies: 1
Tcp:
    114 active connections openings
    2 passive connection openings
    0 failed connection attempts
    12 connection resets received
    0 connections established
    7622 segments received
    7533 segments send out
    68 segments retransmited
    0 bad segments received.
    17 resets sent
Udp:
    287 packets received
    0 packets to unknown port received.
    0 packet receive errors
    279 packets sent
TcpExt:
    7 TCP sockets finished time wait in fast timer
    135 delayed acks sent
    Quick ack mode was activated 26 times
    61 packets directly queued to recvmsg prequeue.
    18364064 packets directly received from backlog
    3912320 packets directly received from prequeue
    2081 packets header predicted
    1525 packets header predicted and directly queued to user
    475 acknowledgments not containing data received
    1311 predicted acknowledgments
    1 times recovered from packet loss due to SACK data
    1 congestion windows fully recovered
    4 congestion windows partially recovered using Hoe heuristic
    13 congestion windows recovered after partial ack
    0 TCP data loss events
    4 timeouts after SACK recovery
    1 fast retransmits
```

```
    47 other TCP timeouts
    22 DSACKs sent for old packets
    1 DSACKs received
    9 connections reset due to early user close
```

Para mostrar solamente las estadísticas originadas por conexiones **TCP**, se utiliza:

```
netstat -s -t
```

Lo anterior puede devolver una salida similar a la siguiente:

```
Tcp:
    114 active connections openings
    2 passive connection openings
    0 failed connection attempts
    12 connection resets received
    0 connections established
    7622 segments received
    7533 segments send out
    68 segments retransmited
    0 bad segments received.
    17 resets sent
TcpExt:
    7 TCP sockets finished time wait in fast timer
    135 delayed acks sent
    Quick ack mode was activated 26 times
    61 packets directly queued to recvmsg prequeue.
    18364064 packets directly received from backlog
    3912320 packets directly received from prequeue
    2081 packets header predicted
    1525 packets header predicted and directly queued to user
    475 acknowledgments not containing data received
    1311 predicted acknowledgments
    1 times recovered from packet loss due to SACK data
    1 congestion windows fully recovered
    4 congestion windows partially recovered using Hoe heuristic
    13 congestion windows recovered after partial ack
    0 TCP data loss events
    4 timeouts after SACK recovery
    1 fast retransmits
    47 other TCP timeouts
    22 DSACKs sent for old packets
    1 DSACKs received
    9 connections reset due to early user close
```

Para mostrar solamente las estadísticas originadas por conexiones **UDP**, se utiliza:

```
netstat -s -u
```

Lo anterior puede devolver una salida similar a la siguiente:

```
Udp:
    287 packets received
    0 packets to unknown port received.
    0 packet receive errors
    279 packets sent
```

Para mostrar la tabla de encaminamientos, se utiliza:

```
netstat -r
```

Lo anterior puede devolver una salida similar a la siguiente:

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.0.0     *               255.255.255.0   U         0 0          0 eth0
192.168.122.0   *               255.255.255.0   U         0 0          0 virbr0
169.254.0.0     *               255.255.0.0     U         0 0          0 eth0
default         192.168.0.254   0.0.0.0         UG        0 0          0 eth0
```

Para mostrar las asignaciones grupos de multidifusión, se utiliza:

```
netstat -g
```

Lo anterior puede devolver una salida similar a la siguiente:

```
IPv6/IPv4 Group Memberships
Interface       RefCnt Group
--------------- ------ ---------------------
lo              1      ALL-SYSTEMS.MCAST.NET
virbr0          1      224.0.0.251
virbr0          1      ALL-SYSTEMS.MCAST.NET
eth0            1      224.0.0.251
eth0            1      ALL-SYSTEMS.MCAST.NET
lo              1      ff02::1
peth0           1      ff02::1
virbr0          1      ff02::1:ff00:0
virbr0          1      ff02::1
vif0.0          1      ff02::1
eth0            1      ff02::1:ff56:18b9
eth0            1      ff02::1
xenbr0          1      ff02::1
vif1.0          1      ff02::1
```

Para mostrar la tabla de interfaces activas en el sistema, se utiliza:

```
netstat -i
```

Lo anterior puede devolver una salida similar a la siguiente:

```
Kernel Interface table
Iface       MTU Met    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0       1500   0     2397      0      0      0     2079      0      0      0 BMRU
lo        16436   0     5780      0      0      0     5780      0      0      0 LRU
peth0      1500   0     3294      0      0      0     2584      0      0      0 BORU
vif0.0     1500   0     2079      0      0      0     2397      0      0      0 BORU
vif1.0     1500   0       45      0      0      0      384      0      0      0 BORU
virbr0     1500   0        0      0      0      0       72      0      0      0 BMRU
xenbr0     1500   0      216      0      0      0        0      0      0      0 BORU
```

41. Uso del mandato ARP.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales (incluyendo su publicación, a través de cualquier medio, por entidades con fines de lucro). c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en castellano. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

41.1. Introducción

41.1.1. Acerca de ARP.

ARP significa **A**ddress **R**esolution **P**rotocol o protocolo de resolución de direcciones. **ARP** se utiliza para **supervisar y modificar** la tabla de asignaciones de direcciones **IP** y direcciones **MAC** (**M**edia **A**ccess **C**ontrol). **ARP** utiliza un cache que consiste en una tabla que almacena las asignaciones entre nivel de enlace de datos y las direcciones IP del nivel de red. El nivel de enlace de datos se encarga de gestionar las direcciones **MAC** y el nivel de red de las direcciones **IP**. **ARP** asocia direcciones **IP** a las direcciones **MAC**, justo a la inversa del protocolo **RARP** que asigna direcciones **MAC** a las direcciones **IP**. Para reducir el número de peticiones **ARP**, cada sistema operativo que implementa el protocolo **ARP** mantiene una cache en la **memoria RAM** de todas las recientes asignaciones.

Puede consultarse el manual detallado respecto del uso del mandato arp ejecutando lo siguiente:

```
man 8 arp
```

El tiempo de duración del cache de la tabla de **ARP** es de 60 segundos. Puede cotejarse este valor examinando el contenido del archivo **/proc/sys/net/ipv4/neigh/default/gc_stale_time**.

```
cat /proc/sys/net/ipv4/neigh/default/gc_stale_time
```

Lo anterior debe devolver el valor 60 en la salida.

Cambiar el valor de la duración del cache de la tabla de ARP puede impedir se desborde ésta cuando se trabaja en redes compuestas por centenares o miles de sistemas que en conjunto hacen demasiadas peticiones ARP que pudieran saturar las capacidades de un servidor.

El valor puede modificarse utilizando el mandato **sysctl** solicitando cambiar el valor de la variable **net.ipv4.neigh.default.gc_stale_time**. En el siguiente ejemplo, se cambia el valor **predeterminado** y el correspondiente a la interfaz **eth0**, a 3600 segundos (1 hora):

```
sysctl -w net.ipv4.neigh.default.gc_stale_time=3600
sysctl -w net.ipv4.neigh.eth0.gc_stale_time=3600
```

Para cotejar que el cambio realizado, ejecute los siguientes dos mandatos:

```
cat /proc/sys/net/ipv4/neigh/default/gc_stale_time
cat /proc/sys/net/ipv4/neigh/eth0/gc_stale_time
```

Lo anterior debe devolver el valor 3600 en la salida para ambos mandatos.

Para que el cambio sea permanente, edite el archivo **/etc/sysctl.conf**:

```
vim /etc/sysctl.conf
```

Y añada al final del archivo el siguiente contenido, conservando un espacio antes y después del signo = (igual), asumiendo que se desea cambiar los valores predeterminado y el correspondiente a la interfaz eth0:

```
net.ipv4.neigh.default.gc_stale_time = 3600
net.ipv4.neigh.eth0.gc_stale_time = 3600
```

41.2. Equipamiento lógico necesario.

El mandato **arp** forma parte del paquete **net-tools**, el cual se instala de modo predeterminado en CentOS, Red Hat™ Enterprise Linux, openSUSE™ y SUSE™ Linux Enterprise, pues se trata de un paquete obligatorio.

41.3. Procedimientos.

Para visualizar el cache **ARP** actual, ejecute lo siguiente.

```
arp -a
```

Lo anterior debe devolver algo similar a lo siguiente, en el caso de tratarse de un único sistema:

```
m254.alcancelibre.org (192.168.1.254) at 00:14:95:97:27:E9 [ether] on eth0
```

Cuando se trata de un servidor que sirve como puerta de enlace para una red de área local, la salida de la tabla puede ser similar a lo siguiente:

```
m051.redlocal.net (10.1.1.51) at 00:13:20:D0:09:1E [ether] on eth1
m046.redlocal.net (10.1.1.46) at 00:0F:1F:B1:71:14 [ether] on eth1
m073.redlocal.net (10.1.1.73) at 00:11:25:F6:93:F1 [ether] on eth1
m070.redlocal.net (10.1.1.70) at 00:11:25:F6:A2:52 [ether] on eth1
m040.redlocal.net (10.1.1.40) at 00:0D:60:6E:27:34 [ether] on eth1
m036.redlocal.net (10.1.1.36) at 00:0D:60:6E:25:FB [ether] on eth1
m011.redlocal.net (10.1.1.11) at 00:11:2F:C7:D0:D7 [ether] on eth1
```

El mandato **arp** acepta varias opciones más. Si se desea visualizar la información en estilo *Linux*, se utiliza sin opciones o bien con la opción -e (redundante, pues es el modo predeterminado). Ejemplo:

```
arp
```

Lo anterior debe devolver una salida similar a la siguiente:

```
Address                  HWtype  HWaddress           Flags Mask            Iface
m051.redlocal.net        ether   00:13:20:D0:09:1E   C                     eth1
m046.redlocal.net        ether   00:0F:1F:B1:71:14   C                     eth1
m073.redlocal.net        ether   00:11:25:F6:A2:52   C                     eth1
m070.redlocal.net        ether   00:11:25:F6:95:8E   C                     eth1
m040.redlocal.net        ether   00:0D:60:6E:26:6F   C                     eth1
m036.redlocal.net        ether   00:11:25:F6:5F:81   C                     eth1
```

Si se desea observar lo anterior en formato numérico, se utiliza la opción -n:

```
arp -n
```

Lo anterior debe devolver una salida similar a la siguiente:

```
Address                  HWtype  HWaddress           Flags Mask            Iface
10.1.1.46                ether   00:0F:1F:B1:71:14   C                     eth1
10.1.1.70                ether   00:11:25:F6:A2:52   C                     eth1
10.1.1.73                ether   00:11:25:F6:93:F1   C                     eth1
10.1.1.40                ether   00:0D:60:6E:27:34   C                     eth1
10.1.1.34                ether   00:0D:60:6E:26:6F   C                     eth1
```

Si se desea especificar una interfaz en particular, se utiliza la opción -i, seguida del nombre de la interfaz. Ejemplo:

```
arp -i eth0
```

Lo anterior debe regresar algo similar a lo siguiente, en el caso de tratarse de un único sistema involucrado:

```
Address                  HWtype  HWaddress           Flags Mask            Iface
m254.alcancelibre.org    ether   00:14:95:97:27:E9   C                     eth0
```

Si se desea añadir un registro manualmente, se puede hacer utilizando la opción -s, seguida del nombre de un anfitrión y la dirección MAC correspondiente. Ejemplo:

```
arp -s m200.redlocal.net 00:08:A1:84:18:AD
```

Si se quiere eliminar un registro de la tabla, sólo se utiliza la opción **-d** seguida del nombre del anfitrión (o dirección IP) que se desea eliminar. Ejemplo:

```
arp -d m200.redlocal.net
```

Para limpiar todo el cache, se puede utilizar un bucle como el siguiente:

```
for i in `arp -n | awk '{print $1}' | grep -v Address`
do
    arp -d $i
done
```

En el guión anterior se pide crear la variable *i* a partir de la salida de la ejecución del mandato **arp** con la opción **-n**, para devolver las direcciones numéricas, mostrando a través del mandato **awk**, sólo la primera columna de la tabla generada y eliminando la cadena de caracteres **Address**. Ésto genera una lista de direcciones IP que se asignan como valores de la variable *i* en el bucle, donde se elimina cada una de estas direcciones IP utilizando **arp -d**.

El objeto de limpiar el cache de **ARP** es permitir corregir los registros de la tabla en ciertos escenarios donde, por ejemplo, un equipo fue encendido con una dirección **IP** que ya esté en uso.

42. Introducción a IPTABLES

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales (incluyendo su publicación, a través de cualquier medio, por entidades con fines de lucro). c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en castellano. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

42.1. Introducción.

42.1.1. Acerca de Iptables y Netfilter.

Netfilter es un conjunto de *ganchos* (**Hooks**, es decir, técnicas de programación que se emplean para crear cadenas de procedimientos como manejador) dentro del núcleo de GNU/Linux y que son utilizados para interceptar y manipular paquetes de red. El componente mejor conocido es el cortafuegos, el cual realiza procesos de filtración de paquetes. Los *ganchos* son también utilizados por un componente que se encarga del **NAT** (acrónimo de **N**etwork **A**ddress **T**ranslation o Traducción de dirección de red). Estos componentes son cargados como módulos del núcleo.

Iptables es el nombre de la herramienta de espacio de usuario (**User Space**, es decir, área de memoria donde todas las aplicaciones, en modo de usuario, pueden ser intercambiadas hacia memoria virtual cuando sea necesario) a través de la cual los administradores crean reglas para cada filtrado de paquetes y módulos de **NAT**. **Iptables** es la herramienta estándar de todas las distribuciones modernas de GNU/Linux.

URL: http://www.netfilter.org/

42.2. Equipamiento lógico necesario.

42.2.1. Instalación a través de yum.

Si utiliza **CentOS 5** y 6, **Red Hat Enterprise Linux 5** o 6, solo se necesita realizar lo siguiente para instalar o actualizar el equipamiento lógico necesario:

```
yum -y install iptables
```

42.3. Procedimientos.

42.3.1. Cadenas.

Las cadenas pueden ser para tráfico entrante (INPUT), tráfico saliente (OUTPUT) o tráfico reenviado (**FORWARD**).

42.3.2. Reglas de destino.

Las reglas de destino pueden ser aceptar conexiones (**ACCEPT**), descartar conexiones (**DROP**), rechazar conexiones (**REJECT**), encaminamiento posterior (**POSTROUTING**), encaminamiento previo (**PREROUTING**), **SNAT**, **NAT**, entre otras.

42.3.3. Políticas por defecto.

Establecen cual es la acción a tomar por defecto ante cualquier tipo de conexión. La opción -P cambia una política para una cadena. En el siguiente ejemplo se descartan (**DROP**) todas las conexiones que ingresen (INPUT), todas las conexiones que se reenvíen (**FORWARD**) y todas las conexiones que salgan (OUTPUT), es decir, se descarta todo el tráfico que entre desde una red pública y el que trate de salir desde la red local.

```
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT
```

42.3.4. Limpieza de reglas específicas.

A fin de poder crear nuevas reglas, se deben borrar las existentes, para el tráfico entrante, tráfico reenviado y tráfico saliente así como el NAT.

```
iptables -F INPUT
iptables -F FORWARD
iptables -F OUTPUT
iptables -F -t nat
```

42.3.5. Reglas específicas.

Las opciones más comunes son:

- -A añade una cadena, la opción -i define una interfaz de tráfico entrante
- -o define una interfaz para trafico saliente
- -j establece una regla de destino del tráfico, que puede ser **ACCEPT**, **DROP** o **REJECT**. La
- -m define que se aplica la regla si hay una coincidencia específica
- --state define una lista separada por comas de distinto tipos de estados de las conexiones (INVALID, ESTABLISHED, NEW, RELATED).
- --to-source define que IP reportar al tráfico externo
- -s define trafico de origen
- -d define tráfico de destino
- --source-port define el puerto desde el que se origina la conexión
- --destination-port define el puerto hacia el que se dirige la conexión
- -t tabla a utilizar, pueden ser nat, filter, mangle o raw.

Ejemplos de reglas.

Reenvío de paquetes desde una interfaz de red local (eth1) hacia una interfaz de red pública (eth0):

```
iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
```

Aceptar reenviar los paquetes que son parte de conexiones existentes (ESTABLISHED) o relacionadas de tráfico entrante desde la interfaz eth1 para tráfico saliente por la interfaz eth0:

```
iptables -A FORWARD -i eth0 -o eth1 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Permitir paquetes en el propio muro cortafuegos para tráfico saliente a través de la interfaz eth0 que son parte de conexiones existentes o relacionadas:

```
iptables -A INPUT -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Permitir (**ACCEPT**) todo el tráfico entrante (INPUT) desde (-**s**) cualquier dirección (0/0) la red local (eth1) y desde el retorno del sistema (lo) hacia (-**d**) cualquier destino (0/0):

```
iptables -A INPUT -i eth1 -s 0/0 -d 0/0 -j ACCEPT
iptables -A INPUT -i lo -s 0/0 -d 0/0 -j ACCEPT
```

Hacer (-j) SNAT para el tráfico saliente (-**o**) a tráves de la interfaz eth0 proveniente desde (-**s**) la red local (192.168.0.0/24) utilizando (--to-source) la dirección IP **w.x.y.z**.

```
iptables -A POSTROUTING -t nat -s 192.168.0.0/24 -o eth0 -j SNAT --to-source x.y.z.c
```

Descartar (**DROP**) todo el tráfico entrante (-**i**) desde la interfaz eth0 que trate de utilizar la dirección IP pública del servidor (**w.x.y.z**), alguna dirección IP de la red local (192.168.0.0/24) o la dirección IP del retorno del sistema (127.0.01)

```
iptables -A INPUT -i eth0 -s w.x.y.x/32 -j DROP
iptables -A INPUT -i eth0 -s 192.168.0.0/24 -j DROP
iptables -A INPUT -i eth0 -s 127.0.0.0/8 -j DROP
```

Aceptar (**ACCEPT**) todos los paquetes SYN (--syn) del protocolo TCP (-p tcp) para los puertos (--**destination-port**) de los protocolos SMTP (25), HTTP(80), HTTPS (443) y SSH (22):

```
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --destination-port 25 --syn -j ACCEPT
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --destination-port 80 --syn -j ACCEPT
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --destination-port 443 --syn -j ACCEPT
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --destination-port 22 --syn -j ACCEPT
```

Aceptar (**ACCEPT**) todos los paquetes SYN (--syn) del protocolo TCP (-tcp) para los puertos (--**destination-port**) del protocolos SMTP (25) en el servidor (**w.x.y.z**/32), desde (-**s**) cualquier lugar (0/0) hacia (-**d**) cualquier lugar (0/0).

```
iptables -A INPUT -p tcp -s 0/0 -d w.x.y.z/32 --destination-port 25 --syn -j ACCEPT
```

Aceptar (**ACCEPT**) todos los paquetes SYN (--syn) del protocolo TCP (-p tcp) para los puertos (--**destination-port**) de los protocolos POP3 (110), POP3S (995), IMAP (143) y IMAPS (993):

```
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --destination-port 110 --syn -j ACCEPT
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --destination-port 995 --syn -j ACCEPT
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --destination-port 143 --syn -j ACCEPT
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --destination-port 993 --syn -j ACCEPT
```

Aceptar (**ACCEPT**) el tráfico entrante (-**i**) proveniente desde la interfaz eth1 cuando las conexiones se establezcan desde el puerto (--sport) 67 por protocolos (-**p**) TCP y UDP.

```
iptables -A INPUT -i eth1 -p tcp --sport 68 --dport 67 -j ACCEPT
iptables -A INPUT -i eth1 -p udp --sport 68 --dport 67 -j ACCEPT
```

Aceptar (**ACCEPT**) conexiones de tráfico entrante (INPUT) por protocolo (-**p**) UDP cuando se establezcan desde (-**s**) el servidor DNS 200.33.145.217 desde el puerto (--**source-port**) 53 hacia (-**d**) cualquier destino (0/0):

```
iptables -A INPUT -p udp -s 200.33.146.217/32 --source-port 53 -d 0/0 -j ACCEPT
```

42.3.5.1. Cerrar accesos.

Descartar (**DROP**) el tráfico entrante (INPUT) para el protocolo (-**p**) TCP hacia los puerto (--**destination-port**) de SSH (22) y Telnet (23):

```
iptables -A INPUT -p tcp --destination-port 22 -j DROP
iptables -A INPUT -p tcp --destination-port 23 -j DROP
```

Descartar (**DROP**) todo tipo de conexiones de tráfico entrante (INPUT) desde (-**s**) la dirección IP a.b.c.d:

```
iptables -A INPUT -s a.b.c.d -j DROP
```

Rechazar (**REJECT**) conexiones hacia (OUTPUT) la dirección IP a.b.c.d desde la red local:

```
iptables -A OUTPUT -d a.b.c.d -s 192.168.0.0/24 -j REJECT
```

42.3.6. Eliminar reglas.

En general se utiliza la misma regla, pero en lugar de utilizar -A (append), se utiliza -D (delete).

Eliminar la regla que descarta (**DROP**) todo tipo de conexiones de tráfico entrante (INPUT) desde (-**s**) la dirección IP a.b.c.d:

```
iptables -D INPUT -s a.b.c.d -j DROP
```

42.3.7. Mostrar la lista de cadenas y reglas.

Una vez cargadas todas las cadenas y reglas de **iptables** es posible visualizar éstas utilizando el mandato **iptables** con las opciones -**n**, para ver las listas en formato numérico y -**L**, para solicitar la lista de éstas cadenas.

```
iptables -nL
```

Cuando no hay reglas ni cadenas cargadas, la salida **debe** devolver lo siguiente:

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Cuando hay cadenas presentes, la salida, suponiendo que se utilizarón los ejemplos de este documento, debe devolver algo similar a lo siguiente:

```
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
DROP       all  --  192.168.1.64         0.0.0.0/0
DROP       all  --  172.16.0.0/24        0.0.0.0/0
DROP       all  --  127.0.0.0/8          0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:25 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:80 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:443 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:22 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            192.168.1.64        tcp dpt:25 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:110 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:995 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:143 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:993 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp spt:68 dpt:67
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp spt:68 dpt:67
ACCEPT     udp  --  200.33.146.217       0.0.0.0/0           udp spt:53

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@m064 ~]# iptables -nL
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
DROP       all  --  192.168.1.64         0.0.0.0/0
DROP       all  --  172.16.0.0/24        0.0.0.0/0
DROP       all  --  127.0.0.0/8          0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:25 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:80 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:443 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:22 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            192.168.1.64        tcp dpt:25 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:110 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:995 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:143 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:993 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp spt:68 dpt:67
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp spt:68 dpt:67
ACCEPT     udp  --  200.33.146.217       0.0.0.0/0           udp spt:53

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

42.3.8. Iniciar, detener y reiniciar el servicio iptables.

Si está de acuerdo con las reglas generadas de **iptables**, utilice el siguiente mandato para guardar éstas:

```
service iptables save
```

Las reglas quedarán almacenadas en el archivo /**etc/sysconfig/iptables**.

Para ejecutar por primera vez el servicio **iptables**, utilice:

```
service iptables start
```

Para hacer que los cambios hechos tras modificar la configuración surtan efecto, utilice:

```
service iptables restart
```

Para detener el servicio **iptables** y borrar todas las reglas utilice:

```
service iptables stop
```

42.3.9. Agregar el servicio iptables al arranque del sistema.

Para hacer que el servicio de **iptables** esté activo con el siguiente inicio del sistema, en todos los niveles de ejecución (2, 3, 4 y 5), se utiliza lo siguiente:

```
chkconfig iptables on
```

42.4. Bibliografía.

- Wikipedia: http://en.wikipedia.org/wiki/Iptables
- Dennis G. Allard y Don Cohen http://oceanpark.com/notes/firewall_example.html

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org/

43. Configuración básica de Shorewall.

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

43.1. Introducción.

43.1.1. Acerca de Shorewall.

Shorewall (Shoreline Firewall) es una robusta y extensible **herramienta de alto nivel para la configuración de muros cortafuego**. **Shorewall** sólo necesita se definan algunos datos en algunos archivos de texto simple y éste creará las reglas de cortafuegos correspondientes a través de **iptables**. **Shorewall** puede permitir utilizar un sistema como muro cortafuegos dedicado, sistema de múltiples funciones como **puerta de enlace, dispositivo de encaminamiento y servidor**.

URL: http://www.shorewall.net/

43.1.2. Acerca de iptables y Netfilter.

Netfilter es un conjunto de *ganchos* (**Hooks**, es decir, técnicas de programación que se emplean para crear cadenas de procedimientos como gestor) dentro del núcleo de GNU/Linux y que son utilizados para interceptar y manipular paquetes de red. El componente mejor conocido es el cortafuegos, el cual realiza procesos de filtración de paquetes. Los *ganchos* son también utilizados por un componente que se encarga del **NAT** (acrónimo de **N**etwork **A**ddress **T**ranslation o Traducción de dirección de red). Estos componentes son cargados como módulos del núcleo.

Iptables es el nombre de la herramienta de espacio de usuario (*User Space*, es decir, área de memoria donde todas las aplicaciones, en modo de usuario, pueden ser intercambiadas hacia memoria virtual cuando sea necesario) a través de la cual los administradores crean reglas para cada filtrado de paquetes y módulos de **NAT**. **Iptables** es la herramienta estándar de todas las distribuciones modernas de GNU/Linux.

URL: http://www.netfilter.org/

43.1.3. Acerca de iproute.

Iproute es una colección de herramientas (ifcfg, ip, rtmon y tc) para GNU/Linux que se utilizan para controlar el establecimiento de la red **TCP/IP**, así como también el control de tráfico. Aunque **ifconfig** sigue siendo la herramienta de configuración de red estándar en las distribuciones de GNU/Linux, **iproute** tiende a sustituirlo al proveer soporte para la mayoría de las tecnologías modernas de red (incluyendo IP versiones 4 y 6), permitiendo a los administradores configurar los parámetros de red y el control de tráfico.

URL: http://linux-net.osdl.org/index.php/Iproute2

43.2. Conceptos requeridos.

43.2.1. ¿Qué es una zona desmilitarizada?

Una zona desmilitarizada (**DMZ**), es parte de una red que no está dentro de la red interna (**LAN**) pero tampoco está directamente conectada hacia Internet. Podría resumirse como una red que se localiza entre dos redes. En términos más técnicos se refiere a un área dentro del cortafuegos donde los sistemas que la componen tienen acceso hacia las redes interna y externa, sin embargo no tienen acceso completo hacia la red interna y tampoco acceso completamente abierto hacia la red externa. Los cortafuegos y dispositivos de encaminamiento (*routers*) protegen esta zona con funcionalidades de filtrado de tráfico de red.

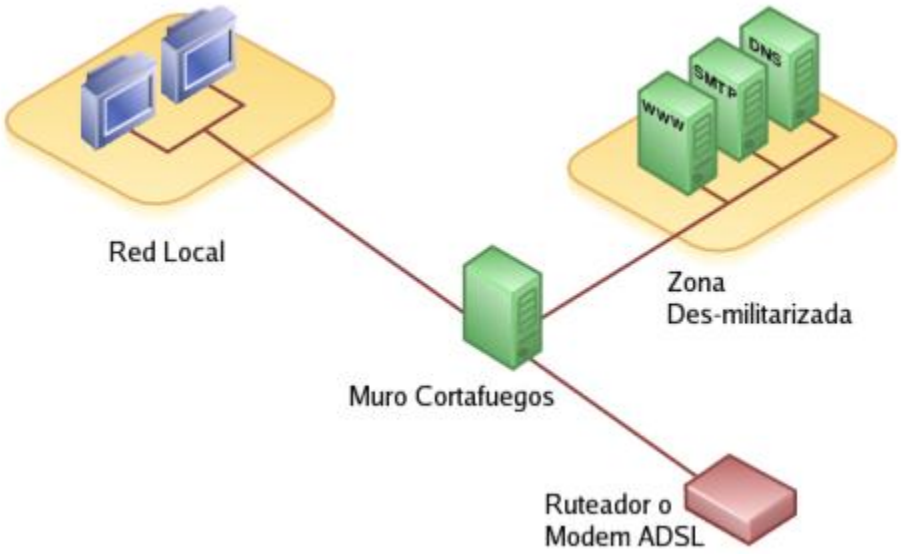


Diagrama de una Zona Desmilitarizada.
Imagen de dominio público tomada de Wikipedia y modificada con el Gimp.

43.2.2. ¿Que es una Red Privada?

Una **Red Privada** es aquella que utiliza direcciones IP establecidas en el RFC 1918. Es decir, direcciones IP reservadas para **Redes Privadas** dentro de los rangos 10.0.0.0/8 (desde 10.0.0.0 hasta 10.255.255.255), 172.16.0.0/12 (desde 172.16.0.0 hasta 172.31.255.255) y 192.168.0.0/16 (desde 192.168.0.0 hasta 192.168.255.255).

43.2.3. ¿Qué es un NAT?

NAT (acrónimo de **N**etwork **A**ddress **T**ranslation o Traducción de dirección de red), también conocido como enmascaramiento de IP, es una técnica mediante la cual las direcciones de origen y/o destino de paquetes IP son reescritas mientras pasan a través de un dispositivo de encaminamiento (*router*) o muro cortafuegos. Se utiliza para permitir a múltiples anfitriones en una **Red Privada** con direcciones IP para **Red Privada** para acceder hacia una Internet utilizando una sola dirección IP pública.

43.2.4. ¿Qué es un DNAT?

DNAT, (acrónimo de **D**estination **N**etwork **A**ddress **T**ranslation o traducción de dirección de red de destino) es una técnica mediante la cual se hace público un servicio desde una **Red Privada**. Es decir permite redirigir puertos hacia direcciones IP de **Red Privada**. El uso de esta técnica puede permitir a un usuario en Internet alcanzar un puerto en una **Red Privada** (dentro de una **LAN**) desde el exterior a través de un encaminador (*router*) o muro cortafuegos donde ha sido habilitado un **NAT**.

43.3. Equipamiento lógico necesario.

- iptables: Controla el código del núcleo de GNU/Linux para filtración de paquetes de red.
- iproute: Conjunto de utilidades diseñadas para utilizar las capacidades avanzadas de gestión de redes del núcleo de GNU/Linux..
- shorewall: Shoreline Firewall.

Shorewall puede descargarse en formato RPM desde http://www.shorewall.net/.

Si dispone de un servidor con **CentOS** o **Red Hat™ Enterprise Linux** puede utilizar el el almacén YUM de **Alcance Libre** ejecutando lo siguiente:

```
cd /etc/yum.repos.d/
wget -N http://www.alcancelibre.org/al/server/AL-Server.repo
cd
```

Ejecute lo siguiente para instalar el paquete **shorewall**:

```
yum -y install shorewall
```

43.4. Procedimientos.

Este documento asume que se han estudiado y aplicado los temas descritos en los documentos titulados «***Ajustes posteriores a la instalación de CentOS 6***» y «***Configuración de red en GNU/Linux***».

43.4.1. Shorewall y SELinux.

Los contextos de SELinux para **/sbin/iptables-multi-1.4.7** y **/sbin/ip6tables-multi-1.4.7** cambiaron del tipo **bin_t** al tipo **iptables_exec_t**. Establezca estos nuevos contextos ejecutando lo siguiente:

```
restorecon -Rv /sbin
```

SELinux impedirá ejecutar algunos componentes de Shorewall instalados en **/usr** e impedirá acceder hacia **/sys** para obtener información respecto de los dispositivos de red presentes en el sistema. El siguiente procedimiento crea una política que permitirá a Shorewall operar normalmente.

Crear el directorio **/usr/share/selinux/packages/shorewall**:

```
mkdir /usr/share/selinux/packages/shorewall
```

Cambiarse al directorio **/usr/share/selinux/packages/shorewall**:

```
cd /usr/share/selinux/packages/shorewall
```

Descargar desde **Alcance Libre** el archivo **http://www.alcancelibre.org/linux/secrets/shorewall.te**:

```
wget http://www.alcancelibre.org/linux/secrets/shorewall.te
```

Editar el archivo **shorewall.te**:

```
vi shorewall.te
```

Verificar que el archivo **shorewall.te** tenga el siguiente contenido:

```
module shorewall 1.0;

require {
        type shorewall_t;
        type usr_t;
        type sysfs_t;
        class file { execute execute_no_trans };
        class dir search;
        class dir getattr;
}

#============= shorewall_t ==============
allow shorewall_t usr_t:file { execute execute_no_trans };
allow shorewall_t sysfs_t:dir search;
allow shorewall_t sysfs_t:dir getattr;
```

Crear el archivo de módulo **shorewall.mod** a partir del archivo **shorewall.te**:

```
checkmodule -M -m -o shorewall.mod shorewall.te
```

Crear el archivo de política **shorewall.pp** a partir del archivo **shorewall.mod**

```
semodule_package -o shorewall.pp -m shorewall.mod
```

Incluir la política al sistema:

```
semodule -i /usr/share/selinux/packages/shorewall/shorewall.pp
```

Regrese al directorio de inicio de root.

```
cd
```

43.4.2. Activación de reenvío de paquetes para IPv4.

Si se dispone de más de un dispositivo de red y se requiere implementar un NAT, DNAT y/o SNAT, es indispensable activar el reenvío de paquetes para IPv4. Edite el archivo **/etc/sysctl.conf**:

```
vi /etc/sysctl.conf
```

Al inicio del archivo encontrará el siguiente contenido:

```
# Kernel sysctl configuration file for Red Hat Linux
#
# For binary values, 0 is disabled, 1 is enabled.  See sysctl(8) and
# sysctl.conf(5) for more details.

# Controls IP packet forwarding
net.ipv4.ip_forward = 0
```

Cambie el valor **0** de **net.ipv4.ip_forward** por **1**:

```
# Kernel sysctl configuration file for Red Hat Linux
#
# For binary values, 0 is disabled, 1 is enabled.  See sysctl(8) and
# sysctl.conf(5) for more details.

# Controls IP packet forwarding
net.ipv4.ip_forward = 1
```

Para aplicar los cambios ejecute lo siguiente:

```
sysctl -p
```

Lo anterior devolverá como salida algo similar a lo siguiente, donde deberá mostrarse que se ha aplicado **net.ipv4.ip_forward** con el valor **1**:

```
net.ipv4.ip_forward = 1
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.default.accept_source_route = 0
kernel.sysrq = 0
kernel.core_uses_pid = 1
error: "net.bridge.bridge-nf-call-ip6tables" is an unknown key
error: "net.bridge.bridge-nf-call-iptables" is an unknown key
error: "net.bridge.bridge-nf-call-arptables" is an unknown key
```

Si se carece de interfaces de red configuradas con IPv6, es normal e inofensivo se muestren los tres errores mostrados arriba.

43.4.3. Procedimiento de configuración de Shorewall.

Se modificarán los siguientes archivos:

- **/etc/shorewall/shorewall.conf**: Archivo general de configuración de Shorewall. En este se activa el servicio y funciones que se requiera utilizar.
- **/etc/shorewall/zones**: Se utiliza para definir las zonas que utilizará el muro cortafuegos.
- **/etc/shorewall/interfaces**: Se utiliza para definir cuáles dispositivos de red corresponden a una zona del muro cortafuegos en particular y las opciones que se requieran para cada una de éstas.
- **/etc/shorewall/masq**: Se utiliza para definir cuáles dispositivos utilizar para los enmascaramientos de direcciones IP.
- **/etc/shorewall/policy**: Se utiliza para definir las políticas predeterminadas para cada zona del muro cortafuegos respecto de las demás zonas.
- **/etc/shorewall/rules**: Se utiliza para definir las reglas para apertura de puertos.
- **/etc/shorewall/blacklist**: Se utiliza para definir las direcciones IP o bloques de direcciones IP que se desea poner en lista negra.

Shorewall viene inactivo de modo predeterminado. Para activar el servicio edite el archivo **/etc/shorewall/shorewall.conf**:

```
vi /etc/shorewall/shorewall.conf
```

Localice la opción **STARTUP_ENABLED**, la cual deberá tener «**No**» como valor predeterminado:

```
STARTUP_ENABLED=No
```

Cambie «**No**» por «**Yes**»:

```
STARTUP_ENABLED=Yes
```

Se requiere definir cuáles zonas serán gestionadas en el muro cortafuegos. Edite el archivo **/etc/shorewall/zones**:

```
vi /etc/shorewall/zones
```

Encontrará que sólo está definida la zona **fw** con el tipo **firewall**:

```
fw      firewall
```

Si dispone de un único dispositivo de red sólo podrá definir una zona (**net**) tipo **ipv4**:

```
fw      firewall
net     ipv4
```

Si dispone de dos dispositivos de red, puede especificar una segunda zona (**loc**) tipo **ipv4**, la cual puede ser utilizada para acceder desde la red de área local:

```
fw      firewall
net     ipv4
loc     ipv4
```

Si dispone de tres dispositivos de red, puede especificar una tercera zona (**dmz**) tipo **ipv4**, la cual puede ser utilizada para acceder desde la zona des-militarizada:

```
fw      firewall
net     ipv4
loc     ipv4
dmz     ipv4
```

Una vez definidas la zonas a utilizar en el muro cortafuegos, se debe definir que dispositivos de red corresponden a cada zona del muro cortafuegos. Edite el archivo **/etc/shorewall/interfaces**:

```
vi /etc/shorewall/interfaces
```

Si dispone de un único dispositivo de red defina el nombre del dispositivo de red a utilizar, auto-detección de la dirección de difusión (**broadcast**) y las opción **blacklist** para utilizar la lista negra de Shorewall y la opción **dhcp**. Esta última opción sólo es necesaria si en la interfaz habrá un cliente o servidor DHCP. El nombre del dispositivo de red puede ser eth0, eth1, p1p1, p2p1, em1, em2, etc., dependiendo de la versión de SMBIOS:

```
net     eth0    detect  blacklist,dhcp
```

Si dispone de un segundo dispositivo de red puede asociar éste a la segunda zona del muro cortafuegos (**loc**). Igualmente defina que se auto-detecte la dirección de difusión y las opciones **blacklist** y **dhcp** si las considera necesarias.

```
net     eth0    detect  blacklist,dhcp
loc     eth1    detect  blacklist,dhcp
```

Si dispone de un tercer dispositivo de red puede asociar éste a la tercera zona del muro cortafuegos (**dmz**). Igualmente defina que se auto-detecte la dirección de difusión y las opciones **blacklist** y **dhcp** si las considera necesarias. Por lo general las zonas des-militarizadas prescinden de servidores DHCP por tratarse de redes designadas para alojar otros servidores con dirección IP estática.

```
net     eth0    detect  blacklist,dhcp
loc     eth1    detect  blacklist,dhcp
dmz     eth2    detect  blacklist
```

Si dispone de un único dispositivo de red, omita el siguiente paso. Si dispone de de más de un dispositivo de red y se requiere habilitar el enmascaramiento de direcciones IP de un dispositivo hacia otro, edite el archivo **/etc/shorewall/masq**:

```
vi /etc/shorewall/masq
```

Si dispone de dos dispositivos de red, defina en la primera columna el dispositivo utilizado para la zona correspondiente a la red pública (**net**) y en la segunda columna el dispositivo utilizado por la zona correspondiente a la red de área local (**loc**):

```
eth0    eth1
```

Si dispone de tres dispositivos de red, añada otra línea donde se defina en la primera columna el dispositivo utilizado para la zona correspondiente a la red pública (**net**) y en la segunda columna el dispositivo utilizado por la zona correspondiente a la zona des-militarizada (**dmz**):

```
eth0    eth1
eth0    eth2
```

Si además de tres dispositivos de red se dispone también de más de una dirección IP en el dispositivo correspondiente a al red pública, puede configurar el **SNAT** (***S**ource **N**etwork **A**ddress **T**ranslation*, mejor conocido en los entornos Windows como ***S**ecure **N**etwork **A**ddress **T**ranslation*) para cada una de las zonas que serán enmascaradas. En el siguiente ejemplo se enmascara todo el tráfico originado desde el dispositivo eth1 con la dirección IP 200.1.2.3 y el tráfico proveniente del dispositivo eth2 con la dirección IP 200.1.2.4.

```
eth0    eth1    200.1.2.3
eth0    eth2    200.1.2.4
```

Edite el archivo **/etc/shorewall/policy**

```
vi /etc/shorewall/policy
```

Si dispone de un sólo dispositivo de red defina sólo dos políticas. Una que permita al muro cortafuegos comunicarse a cualquier parte y otra que descarte cualquier paquete proveniente de la zona de red pública (**net**) y se guarde bitácora de la actividad generada y etiquetada con **DROP**:

```
fw      all     ACCEPT
net     all     DROP    info
```

Si dispone de dos dispositivos de red añada una tercera política que rechace todos los paquetes provenientes desde la zona correspondiente a la red de área local (**loc**) y se guarde bitácora de la actividad generada y etiquetada con **REJECT**:

```
fw      all     ACCEPT
net     all     DROP    info
loc     all     REJECT  info
```

Si dispone de tres dispositivos de red añada una cuarta política que rechace todos los paquetes provenientes desde la zona correspondiente a la zona des-militarizada (**dmz**) y se guarde bitácora de la actividad generada y etiquetada con **REJECT**:

```
fw      all     ACCEPT
net     all     DROP    info
loc     all     REJECT  info
dmz     all     REJECT  info
```

Edite el archivo **/etc/shorewall/rules**:

```
vi /etc/shorewall/rules
```

Debajo de **SECTION NEW** defina una regla que permita el acceso hacia el servicio de SSH (puerto 22/TCP) desde cualquier zona del muro cortafuegos:

```
SECTION NEW
ACCEPT  all     fw      tcp     22
```

Si requiere habilitar más puertos, puede hacerlo añadiendo líneas similares especificando el protocolo utilizado y el puerto o los puertos requeridos. En el siguiente ejemplo se habilitan los puertos para FTP, HTTP, HTTPS y el rango de puertos para conexiones pasivas para el servicio de FTP.

```
SECTION NEW
ACCEPT  all     fw      tcp     22
ACCEPT  all     fw      tcp     20,21,80,443,30300:30309
```

Defina una regla que permita hacer pings (puerto 8/ICMP) hacia el muro cortafuegos desde cualquier zona del muro cortafuegos, sin importar el puerto de origen, sin importar la dirección IP de destino y limitando a una tasa de 10 conexiones por segundo con ráfagas de 5:

```
SECTION NEW
ACCEPT  all     fw      tcp     22
ACCEPT  all     fw      tcp     20,21,80,443,30300:30309
ACCEPT  all     fw      icmp    8       -       -       10/sec:5
```

Si dispone de dos dispositivos de red, puede habilitar la salida desde la zona correspondiente a la red de área local (**loc**) hacia diversos puertos en la zona correspondiente a la red pública (**net**). En el siguiente ejemplo se habilita la salida para los puertos 20 (ftp-data), 21 (ftp), 22 (ssh), 25 (smtp), 43 (whois), 53 (dns), 63 (whois++), 80 (http), 110 (pop3), 123 (ntp), 143 (imap), 443 (https), 465 (smtps), 587 (submission), 993 (imaps) y 995 (pop3s) por TCP, los puertos 43 (whois), 53 (dns), 63 (whois++) y 123 (ntp) por UDP y los pings (puerto 8 por ICMP) limitado a una tasa de 20 conexiones por segundo con ráfagas de 10:

```
SECTION NEW
ACCEPT  all     fw      tcp     22
ACCEPT  all     fw      tcp     20,21,80,443,30300:30309
ACCEPT  all     fw      icmp    8       -       -       10/sec:5
ACCEPT  loc     net     tcp     20,21,80,443
ACCEPT  loc     net     tcp     25,110,143,465,587,993,995
ACCEPT  loc     net     tcp     43,53,63,123
ACCEPT  loc     net     udp     43,53,63,123
ACCEPT  loc     net     icmp    8       -       -       20/sec:10
```

Si dispone de tres dispositivos de red, puede habilitar la salida desde la zona correspondiente a la zona des-militarizada (**dmz**) hacia diversos puertos en la zona correspondiente a la red pública (**net**). En el siguiente ejemplo se habilita la salida para los puertos 20 (ftp-data), 21 (ftp), 22 (ssh), 25 (smtp), 43 (whois), 53 (dns), 63 (whois++), 80 (http), 110 (pop3), 123 (ntp), 143 (imap), 443 (https), 465 (smtps), 587 (submission), 993 (imaps) y 995 (pop3s) por TCP, los puertos 43 (whois), 53 (dns), 63 (whois++) y 123 (ntp) por UDP y los pings (puerto 8 por ICMP) limitado a una tasa de 20 conexiones por segundo con ráfagas de 10:

```
SECTION NEW
ACCEPT  all     fw      tcp     22
ACCEPT  all     fw      tcp     20,21,80,443,30300:30309
ACCEPT  all     fw      icmp    8       -       -       10/sec:5
ACCEPT  loc     net     tcp     20,21,80,443
ACCEPT  loc     net     tcp     25,110,143,465,587,993,995
ACCEPT  loc     net     tcp     43,53,63,123
ACCEPT  loc     net     udp     43,53,63,123
ACCEPT  loc     net     icmp    8       -       -       20/sec:10
ACCEPT  dmz     net     tcp     20,21,80,443
ACCEPT  dmz     net     tcp     25,110,143,465,587,993,995
ACCEPT  dmz     net     tcp     43,53,63,123
ACCEPT  dmz     net     udp     43,53,63,123
ACCEPT  dmz     net     icmp    8       -       -       20/sec:10
```

Edite el archivo /etc/shorewall/blacklist:

```
vi /etc/shorewall/blacklist
```

Cualquier dirección IP o bloques de direcciones IP que se añadan a este archivo quedarán automáticamente en lista negra. Ejemplos de algunos bloques de direcciones asignados a África y algunos de los bloques de direcciones controlados por la mafia rusa:

```
41.0.0.0/8
196.0.0.0/8
154.0.0.0/8
197.0.0.0/8
92.241.160.0/19
91.144.176.0/22
212.191.0.0/17
79.171.80.0/21
```

Al terminar la configuración, inicie el muro cortafuegos ejecutando lo siguiente:

```
service shorewall start
```

Si falla al iniciar, significa que hubo errores de sintaxis en cualquiera de los archivos editados. Revise el contenido de la bitácora de inicio de Shorewall ejecutando lo siguiente:

```
tail -80 /var/log/shorewall-init.log
```

Realice las correcciones pertinentes e intente iniciar de nuevo el servicio.

43.4.4. Iniciar, detener y reiniciar el servicio shorewall.

Para iniciar por primera vez el servicio ejecute lo siguiente:

```
service shorewall start
```

Para reiniciar el servicio **shorewall** o bien hacer que los cambios hechos a la configuración surtan efecto, ejecute lo siguiente:

```
service shorewall restart
```

Para detener el servicio **shorewall**, ejecute lo siguiente:

```
service shorewall stop
```

43.4.5. Agregar el servicio shorewall al arranque del sistema.

De modo predeterminado el servicio **shorewall** viene activo en los niveles de ejecución 2, 3, 4, y 5. Si necesita desactivar el servicio dureante el siguiente inicio del sistema, ejecute lo siguiente:

```
chkconfig shorewall off
```

Para hacer que el servicio de **shorewall** quede nuevamente activo con el siguiente inicio del sistema, ejecute lo siguiente:

```
chkconfig shorewall on
```

44. Cómo instalar y utilizar ClamAV en CentOS

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

44.1. Introducción.

44.1.1. Acerca de ClamAV.

ClamAV es un conjunto de herramientas antivirus, libre y de código fuente abierto, que tiene las siguiente características:

- Distribuido bajo los términos de la Licencia Publica General GNU versión 2.
- Cumple con las especificaciones de familia de estándares **POSIX** (**P**ortable **O**perating **S**ystem **I**nterface for UNI**X** o interfaz portable de sistema operativo para Unix).
- Exploración rápida.
- Detecta más de 720 mil virus, gusanos, troyanos y otros programas maliciosos.
- Capacidad para examinar contenido de archivos ZIP, RAR, Tar, Gzip, Bzip2, MS OLE2, MS Cabinet, MS CHM y MS SZDD.
- Soporte para explorar archivos comprimidos con UPX, FSG y Petite.
- Avanzada herramienta de actualización con soporte para firmas digitales y consultas basadas sobre DNS.

URL: http://www.clamav.net/

44.2. Equipamiento lógico necesario.

- clamav
- clamav-update

44.2.1. Creación del usuario para ClamAV.

De modo predeterminado, el usuario para ClamAV asigna a través de los mandatos **fedora-groupadd** y **fedora-useradd** el UID y GID 4 en el sistema. A fin de prevenir un conflicto de UID/GID con otros usuarios y grupos de sistema, se recomienda crear previamente al grupo y usuario correspondientes para ClamAV:

```
groupadd -r clamavupdate
useradd -r -s /sbin/nologin -d /var/lib/clamav -M -c 'Clamav database update user' \
-g clamavupdate clamavupdate
```

44.2.2. Instalación a través de yum.

Si dispone de un servidor con **CentOS 4** y **5**, **Red Hat™ Enterprise Linux 4** y **5** o **White Box Enterprise Linux 4** y **5**, puede utilizar el el depósito yum de **Alcance Libre** para servidores en producción, creando el archivo **/etc/yum.repos.d/AL-Server.repo** con el siguiente contenido:

```
[AL-Server]
name=AL Server para Enterprise Linux $releasever
mirrorlist=http://www.alcancelibre.org/al/el$releasever/al-server
gpgcheck=1
gpgkey=http://www.alcancelibre.org/al/AL-RPM-KEY
```

La instalación solo requiere utilizar lo siguiente:

```
yum -y install clamav clamav-update
```

La instalación de los paquetes anteriores crea automáticamente el usuario y directorios necesarios para un funcionamiento normal./p>

44.3. Procedimientos.

44.3.1. SELinux y el servicio clamav-milter.

Para que SELinux permita utilizar normalmente **clamscan**, utilice el siguiente mandato:

```
setsebool -P clamscan_disable_trans 1
```

Para que SELinux permita al mandato **freshclam** funcionar normalmente y que permita actualizar la base de datos de firmas digitales, utilice el siguiente mandato:

```
setsebool -P freshclam_disable_trans 1
```

44.3.2. Configuración de Freshclam.

Freshclam es el programa utilizado para descargar y mantener actualizada la base de datos de virus y otros programas malignos.

El archivo **/etc/freshclam.conf** de los paquetes distribuidos por **Alcance Libre** ya incluye las modificaciones necesarias para permitir el funcionamiento del mandato **freshclam**. Sin embargo, si se utilizan paquetes para Fedora, es necesario editar este archivo y comentar o eliminar la línea 9, que incluye simplemente la palabra inglesa *Example* y que de otro mod impediría utilizar el mandato **freshclam**:

```
##
## Example config file for freshclam
## Please read the freshclam.conf(5) manual before editing this file.
##


# Comment or remove the line below.
# Example
```

El archivo **/etc/sysconfig/freshclam** de los paquetes distribuidos por **Alcance Libre** ya incluye las modificaciones necesarias para permitir la actualización automática de la base de datos de **ClamAV**. Si se utilizan paquetes de Fedora y a fin de mantener actualizada la base de datos de firmas digitales, es necesario editar el archivo **/etc/sysconfig/freshclam** con el objeto de permitir las actualizaciones automáticas:

```
### !!!!! REMOVE ME !!!!!!
### REMOVE ME: By default, the freshclam update is disabled to avoid
### REMOVE ME: network access without prior activation
# FRESHCLAM_DELAY=disabled-warn # REMOVE ME
```

De ser necesario, puede actualizar manualmente y de manera inmediata, la base de datos de firmas utilizando el mandato **freshclam**, desde cualquier terminal como **root**.

```
freshclam
```

El paquete de **clamav-update** distribuido por **Alcance Libre** y el proyecto Fedora incluye un guión de actualización automática de la base de datos de ClamAV y que consiste en el archivo **/etc/cron.d/clamav-update**, el cual, a través del servicio **crond**, se ejecuta cada tres horas para verificar si hubo cambios en la base de datos.

44.3.3. Uso básico del mandato clamscan.

para revisar un archivo sospechoso de estar infectado, se utiliza el mandato **clamscan** sin más parámetros:

```
clamscan /cualquier/archivo
```

Para realizar al revisión de un directorio y todo su contenido, es decir, de manera recursiva, se utiliza el mandato **clamscan** con la opción **-r**.

```
clamscan -r /cualquier/directorio
```

Para especificar que los archivos infectados solo sean movidos a un directorio de cuarentena, se utiliza el mandato **clamscan** con la opción **--move** especificando un directorio que servirá como cuarentena. El directorio de cuarentena debe de existir previamente.

```
clamscan --move=/directorio/de/cuarentena -r /cualquier/directorio
```

Para especificar que los archivos infectados sean eliminados, se utiliza la opción **--remove** con el valor **yes**. Esta opción debe ser utilizada con precaución.

```
clamscan --remove=yes -r /cualquier/directorio
```

la salida del mandato **clamscan** puede llegar a ser muy extensa. Si se desea que solo se muestre la información de los archivos infectados, se utiliza el mandato **clamscan** con la opción **--infected**.

```
clamscan --infected --remove=yes -r /cualquier/directorio
```

Para que el mandato **clamscan** guarde la información de su actividad en una bitácora en particular, a fin de poder examinar posteriormente ésta a detalle, se puede utilizar éste con la opción **--log** especificando la ruta de un archivo donde se almacenará la bitácora de actividad.

```
clamscan --log=/home/usuario/clamscan.log --infected --remove=yes -r /cualquier/directorio
```

Para configurar **ClamAV** para ser utilizado con un servidor de correo electrónico con **Sendmail**, consultar el documento titulado «Cómo configurar clamav-milter.»

45. Instalación y configuración de CUPS.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

45.1. Introducción.

45.1.1. Acerca de CUPS.

CUPS (**C**ommon **U**NIX **P**rinting **S**ystem) es un sistema de impresión para GNU/Linux y otros sistemas operativos basados sobre el estándar POSIX, distribuido bajo los términos de la licencia GNU/GPLv2.

Fue originalmente desarrollado en 1997 por Michael Sweet, dueño de Easy Software Products, utilizando en ese entonces el protocolo LPD (Line Printer Daemon protocol), el cual tenía muchas limitaciones técnicas e incompatibilidades entre las diversas marcas de impresoras, motivo por el cual se cambio por **IPP** (**I**nternet **P**rinting **P**rotocol). En 2002 **CUPS** fue incluido por primera vez en Mac OS X, convirtiéndose en el sistema de impresión de facto utilizado hasta la fecha en ese sistema operativo. En febrero de 2007, **Apple Inc.** contrató como empleado a Michael Sweet, comprando además el código fuente de CUPS.

CUPS se compone de una cola de impresión con un planificador, un sistema de filtros para convertir los datos a formatos que puedan utilizar las impresoras y un sistema que permite enviar estos datos hacia la impresora. Permite además utilizar cualquier equipo como servidor de impresión, a través del protocolo **IPP**, utilizando el puerto **631/TCP**.

Los controladores para **CUPS** utilizan el formato **PPD** (**P**ostScript **P**rinter **D**escription), desarrollado por **Adobe Systems** y que consisten en archivos con extensión *.ppd (o bien *.ppd.gz cuando llevan compresión con el algoritmo GZIP), generalmente creados y mantenidos por los fabricantes de impresoras, los cuales contienen el código PostScript necesario para utilizar las características particulares de un modelo de impresora en particular. **CUPS** utiliza este formato para todas las impresoras, incluso las no-PostScript, utilizando filtros que redirigen salidas cuando el caso lo requiere.

CUPS incluye además un conjunto de herramientas para el intérprete de mandatos que permiten la gestión de trabajos de impresión.

45.2. Equipamiento lógico necesario.

45.2.1. En CentOS, Fedora™ y Red Hat Enterprise™ Linux.

Si se realiza una instalación estándar de **CentOS**, **Fedora** o **Red Hat Enterprise Linux**, **CUPS** viene incluido de modo predeterminado. Si se realiza una instalación mínima o bien si durante la instalación se excluyó el soporte para impresión, ejecute lo siguiente lo siguiente:

```
yum -y install cups
```

Si se quiere que **CUPS** disponga de una colección completa de controladores para impresoras, ejecute lo siguiente:

```
yum -y install foomatic-db-ppds gutenprint-cups printer-filters
```

Si instala el paquete **cups-pdf**, dispondrá de una extensión que permitirá crear archivos PDF directamente desde CUPS.

```
yum -y install cups-pdf
```

Si se tienen impresoras multi-funcionales Hewlett-Packard, instale además el paquete **hpijs**.

```
yum -y install hpijs
```

Si requiere una interfaz gráfica estándar, la cual permita la configuración y administración fácil de impresoras y una herramienta que permita descargar automáticamente los controladores que sean necesarios a través de **PackageKit**, instale los paquetes **system-config-printer** y **cups-pk-helper**, ejecutando lo siguiente:

```
yum -y install system-config-printer cups-pk-helper
```

Puede simplificar todo lo anterior ejecutando lo siguiente:

```
yum -y groupinstall print-client print-server
```

45.2.2. En openSUSE™ y SUSE™ Linux Enterprise.

La instalación estándar de openSUSE y SUSE Enterprise Linux incluye cups y todo lo necesario para configurar la mayoría de las impresoras compatibles disponibles. Si se realizó una instalación mínima, instale con yast los paquetes **cups**, **cups-backends**, **cups-client**, **foomatic-filters**, **gutenprint** y **yast2-printer** , ejecutando lo siguiente:

```
yast -i cups cups-backends cups-client foomatic-filters \
    gutenprint yast2-printer
```

El soporte para impresoras multi-funcionales de **Hewlett-Packard** requiere además instalar los paquetes **OpenPrintingPPDs-hpijs** y **hplip-hpijs**. Ejecute lo siguiente:

```
yast -i OpenPrintingPPDs-hpijs hplip-hpijs
```

Al igual que con las otras distribuciones de GNU/Linux, si requiere una interfaz gráfica estándar, la cual permita la configuración y administración fácil de impresoras y una herramienta que permita descargar automáticamente los controladores que sean necesarios a través de **PackageKit**, instale los paquetes **system-config-printer** y **cups-pk-helper**, ejecutando lo siguiente:

```
yast -i system-config-printer cups-pk-helper
```

45.3. Iniciar servicio y añadir el servicio al arranque del sistema.

45.3.1. En CentOS, Fedora™ y Red Hat™ Enterprise Linux.

En éstos el método estándar para iniciar cups es a través del mandato **service**, que también está presente en **openSUSE** y **SUSE Linux Enterprise**.

CUPS es un servicio que sólo es necesario instalar e iniciar para poder ser utilizado. De modo predeterminado se habilita en los niveles de ejecución 2, 3, 4 y 5, por lo cual es innecesario utilizar el mandato **chkconfig**, a menos que sea para desactivar el servicio **cups** en algún de nivel de ejecución en particular.

Ejecute lo siguiente para iniciar el servicio por primera vez:

```
service cups start
```

Cuando el caso lo amerite, ejecute lo siguiente para reiniciar el servicio:

```
service cups restart
```

Ejecute lo siguiente para detener el servicio:

```
service cups stop
```

45.3.2. En openSUSE™ y SUSE™ Linux Enterprise.

Si se utiliza **openSUSE** o **SUSE Linux Enterprise**, el método estándar es través del mandato **rccups**.

Ejecute lo siguiente para iniciar el servicio por primera vez:

```
rccups start
```

Cuando el caso lo amerite, ejecute lo siguiente para reiniciar el servicio:

```
rccups restart
```

Ejecute lo siguiente para detener el servicio:

```
rccups stop
```

45.4. Modificaciones necesarias en el muro cortafuegos.

Para servidores de impresión, es necesario abrir en el muro cortafuegos el puerto 631 **por TCP y UDP** (**IPP**).

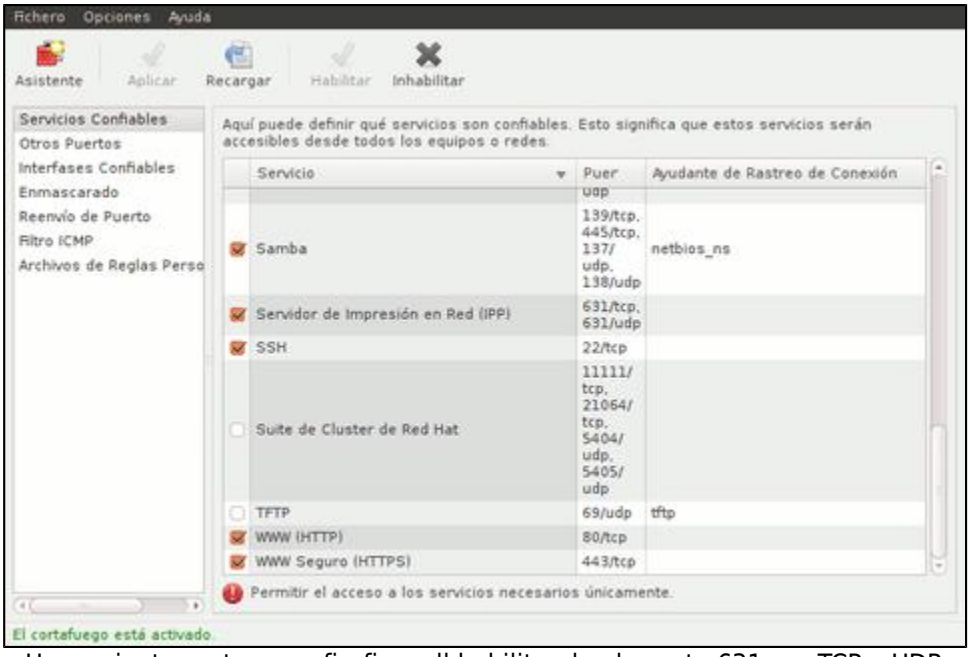
45.4.1. En CentOS, Fedora™ y Red Hat Enterprise™ Linux.

45.4.1.1. System-config-firewall.

Si utiliza el muro cortafuegos predeterminado del sistema, puede ejecutar el siguiente mandato:

```
system-config-firewall
```

Habilite Cliente o Servidor de impresión en red (IPP) —según sea el caso— y aplique los cambios.



Herramienta system-config-firewall habilitando el puerto 631 por TCP y UDP.

45.4.1.2. Servicio iptables.

Puede utilizar directamente el mandato **iptables**, ejecutando lo siguiente:

```
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 631 -j ACCEPT
iptables -A INPUT -m state --state NEW -m udp -p udp --dport 631 -j ACCEPT

service iptables save
```

O bien añada lo siguiente al archivo **/etc/sysconfig/iptables**:

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 631 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 631 -j ACCEPT
```

Y reinicie el servicio **iptables**:

```
service iptables restart
```

Para los clientes del servidor de impresión, sólo es necesario abrir en el muro cortafuegos el puerto 631 **por UDP** (**IPP**).

Utilizado el mandato **iptables**, puede ejecutar lo siguiente:

```
iptables -A INPUT -m state --state NEW -m udp -p udp --dport 631 -j ACCEPT
service iptables save
```

O bien añada lo siguiente al archivo **/etc/sysconfig/iptables**:

```
-A INPUT -m state --state NEW -m udp -p udp --dport 631 -j ACCEPT
```

Y reinicie el servicio **iptables**:

```
service iptables restart
```

45.4.1.3. Shorewall.

Si se va a ser servidor de impresión, las reglas para el archivo **/etc/shorewall/rules** corresponderían a algo similar a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  all     fw      tcp     631
ACCEPT  all     fw      udp     631
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Para los clientes de servidor de impresión, las reglas para el archivo **/etc/shorewall/rules** corresponderían a algo similar a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  all     fw      udp     631
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Para aplicar los cambios, ejecute lo siguiente:

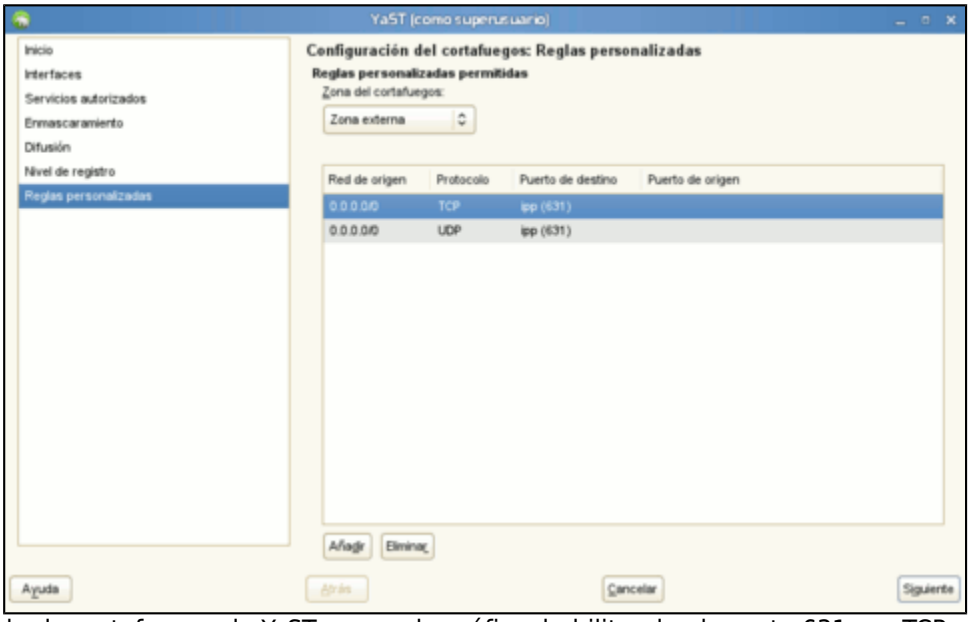
```
service shorewall restart
```

45.4.2. En openSUSE™ y SUSE™ Linux Enterprise.

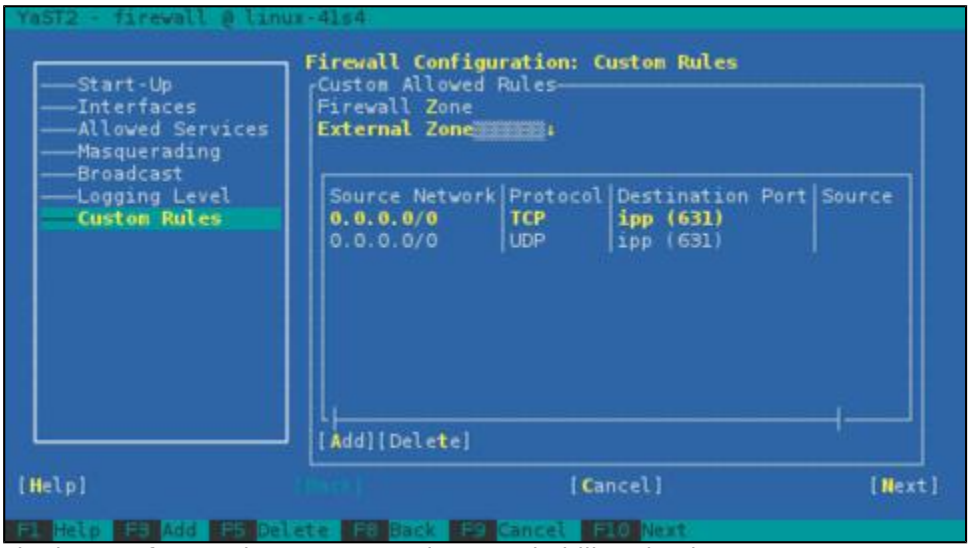
Ejecute el mandato **yast** del siguiente modo:

```
yast firewall
```

Habilite Cliente o Servidor IPP —según sea el caso— o bien abra el puerto 631 por TCP y UDP y aplique los cambios.



Módulo de cortafuegos de YaST, en modo gráfico, habilitando el puerto 631 por TCP y UDP.



Módulo de cortafuegos de YaST, en modo texto, habilitando el puerto 631 por TCP y UDP.

45.5. Archivos y directorios de configuración.

- **/etc/cups/cupsd.conf** se utiliza para configurar las directivas y el control de acceso del servicio **cups**.
- **/etc/cups/printers.conf** se utiliza para guardar la configuración de las colas de impresión.

- **/etc/cups/lpoptions** se utiliza para guardar las opciones de configuración específicas para cada cola de impresión.
- **/etc/cups/ppd/** corresponde al directorio donde se guardan los archivos *.ppd correspondientes a cada cola de impresión.
- **/var/spool/cups/** corresponde al directorio utilizado para la cola de procesamiento de impresión. Aquí se encuentran todos los trabajos de impresión.

Archivos de bitácoras.

- **/var/log/cups/access_log** se utiliza para almacenar la bitácora de actividad del servicio **cups**.
- **/var/log/cups/error_log** se utiliza para almacenar la bitácora de errores del servicio **cups**. Cuando hay problemas con la configuración o el funcionamiento del servicio, este es el archivo indicado para buscar la información necesaria para hacer diagnósticos.
- **/var/log/cups/page_log** se utiliza para almacenar la bitácora de trabajos de impresión.

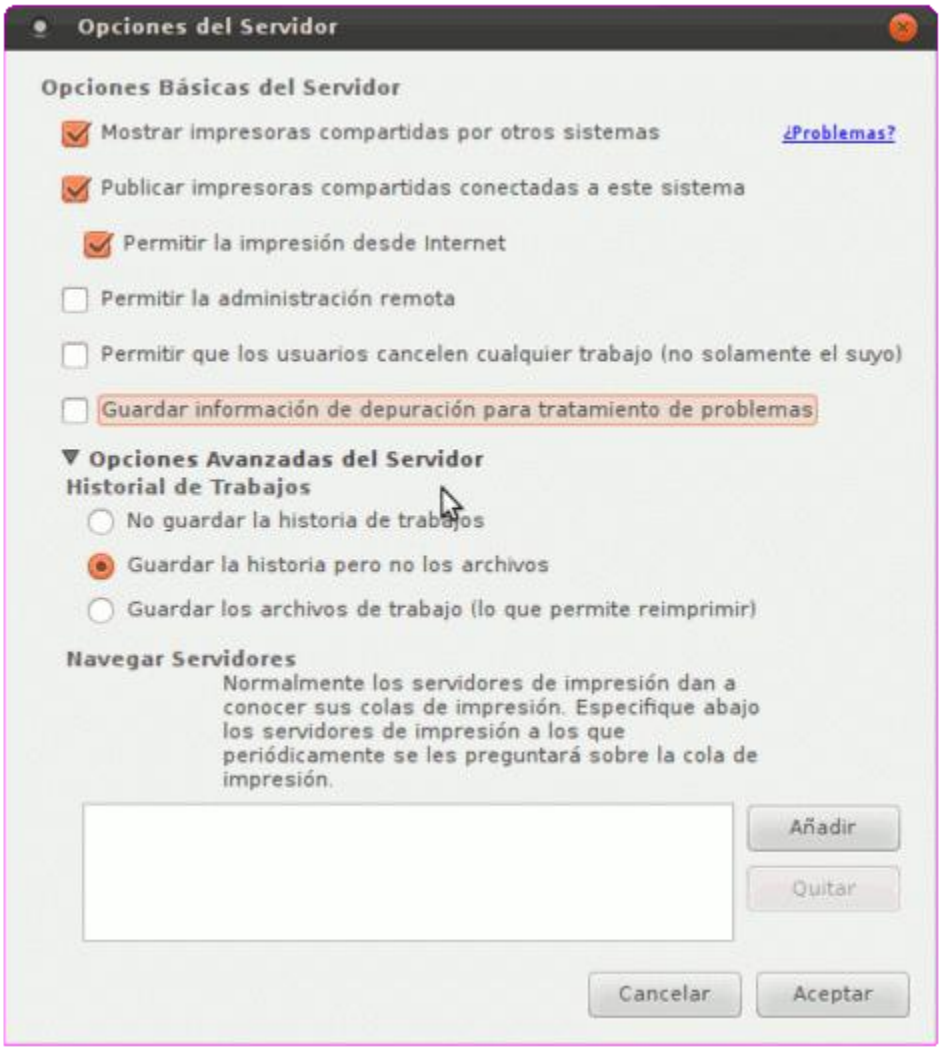
Permitir conexiones desde anfitriones remotos.

De modo predeterminado, el servicio **cups** sólo permite conexiones desde **localhost:631**. Si se requiere compartir las impresoras con el resto de los sistema de la red de área local, se deben hacer algunas modificaciones en la configuración.

45.5.1. En CentOS, Fedora™ o Red Hat Enterprise™.

La herramienta recomendada es **system-config-printer**, sólo disponible desde modo gráfico. Habilite lo siguiente desde *Servidor → Configuración → Opciones del Servidor*:

- Mostrar impresoras compartidas con otros sistemas
- Publicar impresoras compartidas conectadas a este sistema
- Permitir la impresión desde Internet.



Opciones de Servidor de **system-config-printer**.

Al terminar, haga clic en el botón **Aceptar** para que surtan efecto los cambios.

45.5.2. En openSUSE™ o SUSE™ Linux Enterprise.

La herramienta recomendada es el módulo *Impresora* de **YaST**, disponible desde modo gráfico y modo terminal. Habilite lo siguiente desde el menú *Equipo* → *Sistema* → *Yast* → *Impresora* → *Compartir impresoras*:

- Permitir acceso remoto
- Para equipos en la red local
- Publicar las impresoras por defecto en la red local

Módulo de Impresoras de YaST en modo gráfico.

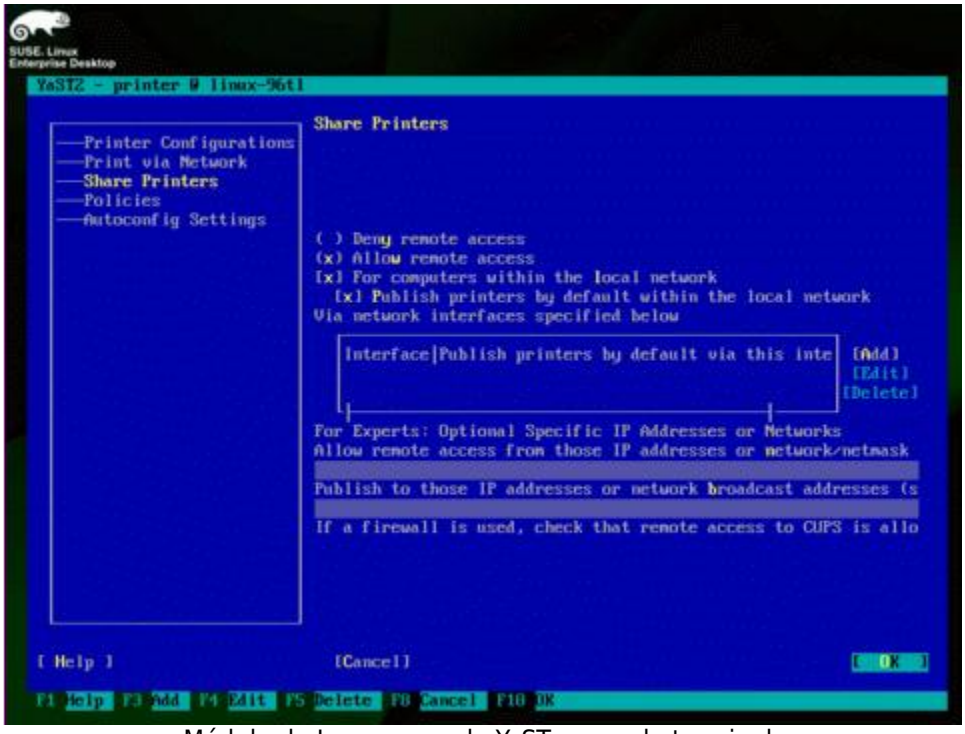
Haga clic en el botón **Aceptar** para que surtan efecto los cambios.

También puede utilizar el módulo *printer* de YaST en modo terminal. Ejecute lo siguiente como root:

```
yast printer
```

Habilite lo siguiente desde *Share Printers*:

- Allow remote access
- For computers within local network
- Publish printers by default within the local network



Módulo de Impresoras de YaST en modo terminal.

Aplique los cambios tabulando hasta *Ok*, pulse la tecla ENTER, espere 20 segundos para que apliquen los cambios y salga del módulo tabulando de nuevo hasta *Ok* y pulse la tecla ENTER.

45.5.3. Modo terminal.

Si utiliza CentOS, Fedora™ o Red Hat Enterprise™ Linux, detenga el servicio **cups** ejecutando lo siguiente:

```
service cups stop
```

Si utiliza openSUSE™ o SUSE™ Linux Enterprise, detenga el servicio **cups** ejecutando lo siguiente:

```
rccups stop
```

Edite el archivo **/etc/cups/cupsd.conf**:

```
vim /etc/cups/cupsd.conf
```

Localice **Listen localhost:631**:

```
# Only listen for connections from the local machine.
Listen localhost:631
```

Deshabilite la opción añadiendo una almohadilla (símbolo **#**) al inicio de la línea y añada debajo **Port 631**:

```
# Only listen for connections from the local machine.
# Listen localhost:631
# Permitir acceso remoto
Port 631
```

Localice lo siguiente:

```
# Show shared printers on the local network.
Browsing On
BrowseOrder allow,deny
BrowseAllow all
BrowseLocalProtocols CUPS dnssd
```

Para habilitar la función de compartir impresoras y el acceso a las impresoras remotas, añada la opción **BrowseRemoteProtocols** con el valor **CUPS** y la opción **BrowseAddress** con el valor **@LOCAL**:

```
# Show shared printers on the local network.
Browsing On
BrowseOrder allow,deny
BrowseAllow all
BrowseRemoteProtocols CUPS
BrowseAddress @LOCAL
BrowseLocalProtocols CUPS dnssd
```

Localice lo siguiente:

```
<Location />
  Order allow,deny
</Location>
```

Añada **Allow all** justo debajo de **Order allow,deny**:

```
<Location />
  Order allow,deny
  Allow all
</Location>
```

Guarde el archivo.

Si utiliza CentOS, Fedora™ o Red Hat Enterprise™ Linux, inicie de nuevo el servicio **cups** ejecutando lo siguiente:

```
service cups start
```

Si utiliza openSUSE™ o SUSE™ Linux Enterprise, inicie de nuevo el servicio **cups** ejecutando lo siguiente:

```
rccups start
```

45.6. Añadir o modificar impresoras.

En la mayoría de las distribuciones modernas y siempre y cuando se trate de un dispositivo compatible, que esté soportado por **CUPS** y que además disponga de un controlador instalado en el sistema, **la configuración de las impresoras es automática**. Sólo se requiere apagar y encender de nuevo la impresora o desconectar y conectar de nuevo ésta para que **CUPS** la detecte y pueda configurar ésta de manera automática.

En el caso que sea necesario, **CUPS** dispone de una interfaz de administración, basada sobre HTTP, disponible inmediatamente después de iniciar el servicio **cups**, a través de **http://localhost:631/admin**. Esta interfaz incluye un asistente de configuración para encontrar y añadir nuevas impresoras o bien administrar las existentes.

En distribuciones como **CentOS**, **Fedora** y **Red Hat Enterprise Linux**, esta interfaz HTTP sólo requiere utilizar la cuenta y clave de acceso del usuario **root** del anfitrión local y sólo está disponible conectándose desde el anfitrión local.

En distribuciones como **openSUSE** y **SUSE Linux Enterprise**, se requiere utilizar el mandato **lppasswd** para añadir un usuario virtual (se recomienda se denomine **cupsadmin**) perteneciente al grupo **sys**, a fin de poder hacer uso de la interfaz HTTP.

```
lppasswd -a -g sys cupsadmin
```

El mandato **lppasswd** almacenará éste y otros usuarios virtuales que se añadan, en el archivo **/etc/cups/passwd.md5**.

Interfaz de administración de **CUPS**.

Para obtener una lista de los modelos de impresoras soportados por **CUPS** y cuyos controladores estén instalados en el sistema dentro del directorio **/usr/share/cups/model**, se ejecuta el mandato **lpinfo** con la opción **-m**:

```
lpinfo -m
```

Para añadir o modificar una impresora desde el intérprete de mandatos, se ejecuta el mandato **lpadmin** del siguiente modo:

```
lpadmin -p Nombre -E -v URI://ruta/nombre -m ppd-impresora
```

Donde:

- **-p** se utiliza para definir el nombre que utilizará **CUPS** para la impresora que se está añadiendo o modificando.
- **-E** define que la cola de impresión está habilitada y que estará compartida con otros anfitriones de la red de área local. Equivale a ejecutar los mandatos **cupsaccept** y **cupsenable** con el nombre de la cola de impresión como argumento.
- **-v** se utiliza para definir el URI (***U**niform **R**esource **I**dentifier* o identificador uniforme de recurso) que corresponda a la cola de impresión.
- **-m** se utiliza para definir el archivo *.ppd a utilizar, de acuerdo a la nomenclatura de la lista mostrada por el mandato **lpinfo -m**.

En lugar de la opción **-m**, puede utilizarse la opción **-P** (mayúscula) para definir archivos *.ppd específicos que hayan sido descargados desde **OpenPrinting** (antes LinuxPrinting.org).

```
lpadmin -p Nombre -E -v URI://ruta/nombre -P archivo.ppd
```

Los URI permitidos por **CUPS** para dispositivos locales son: hp, hpfax, scsi y usb.

Los URI permitidos por **CUPS** para impresoras en red son: beh, http, https, ipp, lpd, smb y socket.

La configuración de las impresoras se guardará en el archivo **/etc/cups/printers.conf**. Si se requiere hacer modificaciones manuales, este archivo puede modificarse con editor de texto sólo cuando el servicio **cups** está detenido, pues de otro modo se perderán los cambios realizados con editor de texto.

Los archivos *.ppd que se definan con la interfaz HTTP de **CUPS**, la herramienta **system-config-printer** o bien el mandato **lpadmin**, se copiarán automáticamente dentro del directorio **/etc/cups/ppd/**.

En el siguiente ejemplo, se añade y/o modifica la configuración para una impresora EPSON EPL-5900, conectada al anfitrión local por USB, utilizando la nomenclatura del archivo *.ppd, mostrada por el mandato **lpinfo -m** y que corresponde al controlador recomendado para este modelo específico de impresora:

```
lpadmin -p EPL-5900 -E \
    -v usb://EPSON/EPL-5900 \
    -m foomatic:Epson-EPL-5900-eplaser.ppd
```

En el siguiente ejemplo, se añade y/o modifica la configuración para la misma impresora, conectada al anfitrión local por USB, utilizando el archivo epl5900.ppd, descargado desde **OpenPrinting**:

```
lpadmin -p EPL-5900 -E \
    -v usb://EPSON/EPL-5900 \
    -P ~/Descargas/epl5900.ppd
```

En el siguiente ejemplo, se añade y/o modifica la configuración para la misma impresora, pero conectada en el servidor IPP con dirección IP 192.168.70.2:

```
lpadmin -p EPL-5900 -E \
    -v ipp://192.168.70.2/printers/EPL-5900 \
    -m foomatic:Epson-EPL-5900-eplaser.ppd
```

En el siguiente ejemplo, se añade y/o modifica la configuración para la misma impresora, pero conectada en el servidor SMB (o bien compartida desde un anfitrión Windows) con dirección IP 192.168.70.2, accediendo como usuario invitado:

```
lpadmin -p EPL-5900 -E \
    -v smb://servidor/printers/EPL-5900 \
    -m foomatic:Epson-EPL-5900-eplaser.ppd
```

En el siguiente ejemplo, se añade y/o modifica la configuración para la misma impresora, pero conectada en el servidor SMB (o bien compartida desde un anfitrión Windows) con dirección IP 192.168.70.2, accediendo con el usuario fulano con clave de acceso 123qwe:

```
lpadmin -p EPL-5900 -E \
    -v smb://fulano:123qwe@servidor/printers/EPL-5900 \
    -m foomatic:Epson-EPL-5900-eplaser.ppd
```

En el caso de haber más de una impresora configurada en **CUPS**, puede establecerse la impresora predeterminada del sistema ejecutando el mandato **lpadmin**, con la opción **-d** y el nombre de la cola de impresión como argumento, como se muestra en el siguiente ejemplo:

```
lpadmin -d EPL-5900
```

Para eliminar una impresora de **CUPS**, se ejecuta el mandato **lpadmin** con la opción **-x**, usando como argumento el nombre de la cola de impresión a eliminar.

```
lpadmin -x EPL-5900
```

45.6.1. Configuración de opciones de impresión.

Las opciones definidas con el mandato **lpoptions** se guardan en el archivo **/etc/cups/lpoptions**. El mandato **lpoptions** puede ser utilizado también por usuarios regulares, pero las opciones definidas por éstos se guardarán en el archivo **~/.cups/lpoptions** (**CentOS**, **Fedora™** o **Red Hat™ Enterprise Linux**) o **~/.lpoptions** (**openSUSE™** y **SUSE™ Linux Enterprise**) del usuario utilizado.

Las opciones disponibles para cada modelo de impresora pueden consultarse y verificarse ejecutando el mandato **lpoptions** con la opción **-l**.

```
lpoptions -p EPL-5900 -l
```

En el caso de la impresora EPSON EPL-5900, lo anterior mostrará una salida similar a la siguiente:

```
PageSize/Page Size: Custom.WIDTHxHEIGHT *Letter A4 A5 B5 Env10 EnvC5 EnvDL EnvISOB5 EnvMonarch
Executive Legal
InputSlot/Paper Source: Tray1 Tray2 Tray3 Tray4 Tray5 Tray6 Tray7 Tray8 Tray9 Tray10 Tray11 Tray12
Tray13 Tray14 Tray15 *Auto
Resolution/Resolution: 300x300dpi *600x600dpi 1200x1200dpi
Copies/Number of Copies: *1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28
29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62
63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96
97 98 99 100 Custom.INTEGER
MediaType/Media Type: *Plain Thick Trans
Duplex/Double-Sided Printing: DuplexNoTumble DuplexTumble *None
Manual/Manual Feed of Paper: True *False
TonerSaving/Economy Mode: True *False
Collate/Output Order: True *False
Landscape/Orientation: True *False
RITOff/RIT Control: True *False
```

La salida se interpreta de la siguiente forma, donde los valores predeterminados se muestran junto con un asterisco:

```
NombreOpción/Descripción de la opción: valores *predeterminado
```

El valor predeterminado para el tamaño del papel, en la mayoría de los controladores, es **A4**. En el siguiente ejemplo se establecerá que de modo predeterminado se utilicé tamaño **carta** para el tamaño del papel, en lugar del valor predeterminado del archivo *.ppd correspondiente, ejecutando el mandato **lpoptions** del siguiente modo:

```
lpoptions -p EPL-5900 -o PageSize=Letter
```

En el siguiente ejemplo se establecerá que, de modo predeterminado, esta impresora utilice tamaño carta para el tamaño del papel, pero modificando del valor predeterminado del archivo *.ppd correspondiente, el cual está dentro del directorio **/etc/cups/ppd/**, ejecutando el mandato **lpadmin** del siguiente modo:

```
lpadmin -p EPL-5900 -o PageSize=Letter
```

En el siguiente ejemplo se establecerá que, de modo predeterminado, se utilice tamaño oficio para el tamaño del papel, en lugar del valor predeterminado del archivo *.ppd correspondiente, ejecutando el mandato **lpoptions** del siguiente modo:

```
lpoptions -p EPL-5900 -o PageSize=Legal
```

En el siguiente ejemplo se establecerá 300x300dpi como valor predeterminado para la resolución de las impresiones:

```
lpoptions -p EPL-5900 -o Resolution=300x300dpi
```

45.7. Impresión desde el intérprete de mandatos.

El estilo ***System V***, que es el método preferido, utiliza el mandato **lp** con la opción **-d** y el nombre de la cola de impresión como argumento.

```
lp -d NombreCola archivo.ps
```

Para hacer la impresión de archivos locales en una impresora remota ejecutando el mandato **lp**, se ejecuta lo anterior con la opción **-h** y el nombre o dirección IP del servidor como argumento.

```
lp -d NombreCola -h 192.168.70.2 archivo.ps
```

El mandato **lp** permite además especificar opciones de impresión cuando el caso lo requiera. En el siguiente ejemplo se realiza la impresión de un archivo en una impresora local, definiendo tamaño oficio para el tamaño del papel:

```
lp -d NombreCola -o PageSize=Legal archivo.ps
```

El estilo ***Berkely***, que es el método antiguo, utiliza el mandato **lpr** con la opción **-P** (mayúscula) y el nombre de la cola de impresión como argumento:

```
lpr -P NombreCola archivo.ps
```

Para hacer la impresión de archivos locales en una impresora remota ejecutando el mandato **lpr**, se ejecuta lo anterior con la opción **-H** (mayúscula) y el nombre o dirección IP del servidor como argumento:

```
lpr -P NombreCola -H 192.168.70.2 archivo.ps
```

El mandato **lpr** también permite especificar opciones de impresión cuando el caso lo requiera. En el siguiente ejemplo se realiza la impresión de un archivo en una impresora local, definiendo tamaño oficio para el tamaño del papel:

```
lpr -P NombreCola -o PageSize=Legal archivo.ps
```

45.8. Verificar estados de las colas de impresión.

Para mostrar el estado de todas las colas de impresión del sistema, utilizando el estilo ***System V***, ejecute el mandato **lpstat** con la opción **-p**:

```
lpstat -p
```

Para mostrar el estado de una impresora en particular, ejecute el mandato **lpstat** con la opción **-p** con el nombre de la cola de impresión como argumento:

```
lpstat -p NombreCola
```

Para mostrar el estado de una impresora en particular en un servidor remoto (por ejemplo 192.168.70.2), ejecute el mandato **lpstat** con la opción **-p** con el nombre de la cola de impresión como argumento y la opción **-h** con el nombre del servidor o la dirección IP correspondiente como argumento:

```
lpstat -p NombreCola -h 192.168.70.2
```

Para mostrar el estado de todos los trabajos de impresión pendientes en todas las colas de impresión del sistema, ejecute el mandato **lpstat** con la opción **-o**:

```
lpstat -o
```

Para mostrar el estado de todos los trabajos de impresión pendientes en una impresora en particular, ejecute el mandato **lpstat** con la opción **-o** con el nombre de la cola de impresión como argumento:

```
lpstat -o NombreCola
```

Para mostrar el estado de una impresora en particular, así como también el estado de todos los trabajos de impresión pendientes en ésta, ejecute el mandato **lpstat** con la opción **-p** con el nombre de la cola de impresión como argumento y la opción **-o** con el nombre de la cola de impresión como argumento.

```
lpstat -p NombreCola -o NombreCola
```

Si se desea información más detallada, ejecute el mandato **lpstat** con la opción **-t**:

```
lpstat -t
```

Si se desea el máximo de información disponible, ejecute el mandato **lpstat** con la opción **-t** y la opción **-l**:

```
lpstat -t -l
```

Para mostrar el estado de todas las colas de impresión del sistema y los trabajos pendientes, utilizando el estilo ***Berkeley***, ejecute el mandato **lpq**:

```
lpq
```

Para mostrar el estado de una impresora en particular, ejecute el mandato **lpq** con la opción **-P** (mayúscula) con el nombre de la cola de impresión como argumento:

```
lpq -PNombreCola
```

Para mostrar el estado de todos los trabajos de impresión pendientes en todas las colas de impresión del sistema, ejecute el mandato **lpq** con la opción **-a**:

```
lpq -a
```

45.8.1. Cancelación de trabajos de impresión.

El estilo ***System V*** utiliza el mandato **cancel** con el nombre de la cola de impresión y el número de trabajo como argumentos.

```
cancel NombreCola-número
```

En el siguiente ejemplo se cancela el trabajo de impresión 5 en la cola de impresión EPL-5900:

```
cancel EPL-5900-5
```

Para eliminar un trabajo de impresión en un servidor remoto, a lo anterior se le añade la opción **-h** con el nombre o dirección IP que corresponda como argumento.

```
cancel -h servidor NombreCola-número
```

En el siguiente ejemplo se cancela el trabajo de impresión 5 en la cola de impresión EPL-5900 en el servidor 192.168.70.2:

```
cancel -h 192.168.70.2 EPL-5900-5
```

El estilo ***Berkeley*** utiliza el mandato **lprm**, la opción **-P** (mayúscula), seguida inmediatamente del nombre de la cola de impresión como argumento y el número del trabajo de impresión que se quiere cancelar:

```
lprm -PNombreCola Número
```

En el siguiente ejemplo se cancela el trabajo de impresión 5 en la cola de impresión EPL-5900:

```
lprm -PEPL-5900 5
```

Para eliminar un trabajo de impresión en un servidor remoto, a lo anterior se le añade la opción **-h** con el nombre o dirección IP que corresponda como argumento.

```
lprm -h servidor -PNombreCola Número
```

En el siguiente ejemplo se cancela el trabajo de impresión 5 en la cola de impresión EPL-5900 en el servidor 192.168.70.2:

```
lprm -h 192.168.70.2 -PEPL-5900 5
```

46. Introducción al protocolo DNS.

Autor: *Joel Barrios Dueña*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

46.1. Equipamiento lógico necesario.

Instale los paquetes **bind-utils** y **jwhois**.

```
yum -y install bind-utils jwhois
```

46.2. Conceptos.

46.2.1. Acerca del protocolo DNS (Domain Name System).

DNS (acrónimo de **D**omain **N**ame **S**ystem) es una base de datos distribuida y jerárquica, que almacena la información necesaria para los nombres de dominio. Sus usos principales son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico correspondientes para cada dominio. El **DNS** nació de la necesidad de facilitar a los seres humanos el acceso hacia los servidores disponibles a través de Internet permitiendo hacerlo por un nombre, algo más fácil de recordar que una dirección **IP**.

Los **Servidores DNS** utilizan **TCP** y **UDP**, en el puerto 53 para responder las consultas. Casi todas las consultas consisten de una sola solicitud **UDP** desde un **Cliente DNS**, seguida por una sola respuesta **UDP** del servidor. Se realiza una conexión **TCP** cuando el tamaño de los datos de la respuesta exceden los 512 bytes, tal como ocurre con tareas como **transferencia de zonas**.

46.2.2. ¿Qué es un NIC (Network Information Center)?

NIC (acrónimo de **N**etwork **I**nformation **C**enter o Centro de Información sobre la Red) es una institución encargada de asignar los nombres de dominio en Internet ya sean nombres de dominio genéricos o por países, permitiendo personas o empresas, montar sitios de Internet a través de un **ISP**, mediante un DNS. Técnicamente existe un **NIC** por cada país en el mundo y cada uno de éstos es responsable por todos los dominios con la terminación correspondiente a su país. Por ejemplo: NIC México es la entidad encargada de gestionar todos los dominios con terminación **.mx**, la cual es la terminación correspondiente asignada a los dominios de México.

46.2.3. ¿Qué es un FQDN (Fully Qualified Domain Name)?

FQDN (acrónimo de **F**ully **Q**ualified **D**omain **N**ame o Nombre de Dominio Plenamente Calificado) es un Nombre de Dominio ambiguo que especifica la posición absoluta del nodo en el árbol jerárquico del DNS. Se distingue de un nombre regular porque lleva un punto al final.

Como ejemplo: suponiendo que se tiene un dispositivo cuyo nombre de anfitrión es «maquina1» y un dominio llamado «dominio.com», el **FQDN** sería «**maquina1.dominio.com.**», así es que se define de forma única al dispositivo mientras que pudieran existir muchos anfitriones llamados «maquina1», solamente puede haber uno llamado «**maquina1.dominio.com.**». La ausencia del punto al final definiría que se pudiera tratar solamente de un prefijo, es decir «**maquina1.dominio.com**» pudiera ser un dominio de otro más largo como «**maquina1.dominio.com.mx**».

La longitud máxima de un **FQDN** es de 255 bytes, con una restricción adicional de 63 bytes para cada etiqueta dentro del nombre del dominio. Solamente se permiten los caracteres A-Z de ASCII, dígitos y el carácter «-» (guión medio). Sin distinción de mayúsculas y minúsculas.

Desde 2004, a solicitud de varios países de Europa, existe el estándar **IDN** (acrónimo de **I**nternationalized **D**omain **N**ame) que permite caracteres no-ASCII, codificando caracteres ***Unicode*** dentro de cadenas de *bytes* dentro del conjunto normal de caracteres de **FQDN**. Como resultado, los limites de longitud de los nombres de dominio **IDN** dependen directamente del contenido mismo del nombre.

46.2.4. Componentes de DNS.

DNS opera a través de tres componentes: Clientes DNS, Servidores DNS y Zonas de Autoridad.

46.2.4.1. Clientes DNS.

Son programas que ejecuta un usuario y que generan peticiones de consulta para resolver nombres. Básicamente preguntan por la dirección IP que corresponde a un nombre determinado.

46.2.4.2. Servidores DNS.

Son servicios que contestan las consultas realizadas por los **Clientes DNS**. Hay dos tipos de servidores de nombres:

- **Servidor Maestro**: También denominado **Primario**. Obtiene los datos del dominio a partir de un archivo alojado en el mismo servidor.
- **Servidor Esclavo**: También denominado **Secundario**. Al iniciar obtiene los datos del dominio a través de un Servidor Maestro (o primario), realizando un proceso denominado **transferencia de zona**.

Un gran número de problemas de operación de servidores DNS se atribuyen a las pobres opciones de servidores secundarios para las zona de DNS. De acuerdo al **RFC 2182**, el DNS requiere que **al menos tres servidores existan** para todos los dominios delegados (o zonas).

Una de las principales razones para **tener al menos tres servidores** para cada zona, es permitir que la información de la zona misma esté disponible siempre y de forma confiable, hacia los **Clientes DNS**, a través de Internet cuando un servidor DNS de dicha zona falle, esté fuera de servicio y/o esté inalcanzable.

Contar con múltiples servidores también facilita la **propagación** de la zona y mejoran la eficiencia del sistema en general al brindar opciones a los **Clientes DNS** si acaso encontraran dificultades para realizar una consulta en un **Servidor DNS**. En otras palabras: tener múltiples servidores para una zona permite **contar con redundancia y respaldo, del servicio**.

Con múltiples servidores, por lo general uno actúa como **Servidor Maestro o Primario** y los demás como **Servidores Esclavos o Secundarios**. Correctamente configurados y una vez creados los datos para una zona, es innecesario copiarlos a cada **Servidor Esclavo o Secundario**, pues éste se encargará de transferir los datos de manera automática cada vez que sea necesario.

Los **Servidores DNS** responden dos tipos de consultas:

- **Consultas Iterativas (no recursivas)**: El cliente hace una consulta al **Servidor DNS** y éste le responde con la mejor respuesta que pueda darse basada sobre su caché o en las zonas locales. Si es imposible dar una respuesta, la consulta se reenvía hacia otro Servidor DNS repitiéndose este proceso hasta encontrar al **Servidor DNS** que tiene la **Zona de Autoridad** capaz de resolver la consulta.
- **Consultas Recursivas**: El **Servidor DNS** asume toda la carga de proporcionar una respuesta completa para la consulta realizada por el **Cliente DNS**. El **Servidor DNS** desarrolla entonces **Consultas Iterativas** separadas hacia otros **Servidores DNS** (en lugar de hacerlo el **Cliente DNS**) para obtener la respuesta solicitada.

46.2.4.3. Zonas de Autoridad.

Permiten al **Servidor Maestro o Primario** cargar la información de una zona. Cada **Zona de Autoridad** abarca al menos un dominio y, posiblemente, sus sub-dominios, si estos últimos son imposibles de delegar a otras zonas de autoridad.

La información de cada **Zona de Autoridad** es almacenada de forma local en un archivo en el **Servidor DNS**. Este archivo puede incluir varios tipos de registros:

Tipo de Registro.	Descripción.
A (**A**ddress)	Registro de dirección que resuelve un nombre de un anfitrión hacia una dirección **IPv4** de 32 bits.
AAAA	Registro de dirección que resuelve un nombre de un anfitrión hacia una dirección **IPv6** de 128 bits.
CNAME (**C**anonical **Name**)	Registro de nombre canónico que hace que un nombre sea alias de otro. Los dominios con alias obtienen los sub-dominios y registros DNS del dominio original.
MX (**M**ail E**x**changer)	Registro de servidor de correo que sirve para definir una lista de servidores de correo para un dominio, así como la prioridad entre éstos.
PTR (**P**oin**t**e**r**)	Registro de apuntador que resuelve direcciones **IPv4** hacia los nombres anfitriones. Es decir, hace lo contrario al registro **A**. Se utiliza en zonas de **Resolución Inversa**.
NS (**N**ame **S**erver)	Registro de servidor de nombres, que sirve para definir una lista de servidores de nombres con autoridad para un dominio.
SOA (**S**tart **of A**uthority)	Registro de inicio de autoridad, encargado de especificar el **Servidor DNS** Maestro (o Primario) que proporcionará la información con autoridad acerca de un dominio de Internet, dirección de correo electrónico del administrador, número de serie del dominio y parámetros de tiempo para la zona.
SRV (**S**e**rv**ice)	Registros de servicios, encargados de especificar información acerca de servicios disponibles a través del dominio. Protocolos como **SIP** (**S**ession **I**nitiation **P**rotocol) y **XMPP** (E**x**tensible **M**essaging and **P**resence **P**rotocol) suelen requerir registros **SRV** en la zona para proporcionar información a los clientes.
TXT (**T**e**xt**)	Registros de texto, encargados de permitir al administrador insertar texto arbitrariamente en un registro DNS. Este tipo de registro es muy utilizado por los servidores de listas negras **DNSBL** (**DNS**-based **B**lackhole **L**ist) para la filtración de Spam. Otro ejemplo de uso sería el caso de las VPN, donde suele requerirse un registro **TXT**, para definir una firma digital que será utilizada por los clientes.

Las zonas que se pueden resolver son:

Zonas de Reenvío.

Devuelven **direcciones IP** para las búsquedas hechas para nombres **FQDN** (**F**ully **Q**ualified **D**omain **N**ame).

En el caso de dominios públicos, la responsabilidad de que exista una **Zona de Autoridad** para cada **Zona de Reenvío**, corresponde a la autoridad misma del dominio, es decir quien esté registrado como autoridad del dominio la base de datos **WHOIS** donde esté registrado el dominio. Quienes adquieren dominios a través de un **NIC** (por ejemplo: www.nic.mx), son quienes deben hacerse cargo de las **Zonas de Reenvío** ya sea a través de su propio **Servidor DNS** o bien a través de los **Servidores DNS** de su **ISP**.

Salvo que se trate de un dominio para uso en una red local, todo dominio debe ser primero tramitado con un **NIC**, como requisito para tener derecho legal a utilizarlo y poder propagarlo a través de Internet.

Zonas de Resolución Inversa.

Devuelven nombres **FQDN** (**F**ully **Q**ualified **D**omain **N**ame) para las búsquedas hechas para **direcciones IP**.

En el caso de segmentos de red públicos, la responsabilidad de que exista una **Zona de Autoridad** para cada **Zona de Resolución Inversa**, corresponde a la autoridad misma del segmento, es decir, corresponde a quien esté registrado como autoridad del bloque de direcciones IP, información que puede ser obtenida al consultar una base de datos **WHOIS**.

Los grandes **ISP** y algunas empresas son quienes se hacen cargo de las **Zonas de Resolución Inversa**.

46.2.5. Herramientas de búsqueda y consulta.

46.2.5.1. Mandato host.

El mandato **host** es una herramienta simple para hacer consultas en **Servidores DNS**. Es utilizado para obtener las direcciones IP de los nombres de anfitrión y viceversa.

De modo predeterminado, realiza las consultas en los **Servidores DNS** que estén definidos en el archivo **/etc/resolv.conf** del anfitrión local, pudiendo definirse de manera opcional cualquier otro **Servidor DNS**.

```
host www.alcancelibre.org
```

Lo anterior realiza una búsqueda en los **Servidores DNS** definidos en el archivo **/etc/resolv.conf** del sistema, devolviendo como resultado una dirección IP.

```
host www.alcancelibre.org 8.8.8.8
```

Lo anterior realiza una búsqueda en los **Servidor DNS** en la dirección IP 8.8.8.8, devolviendo una dirección IP como resultado.

46.2.5.2. Mandato dig.

El mandato **dig** (**d**omain **i**nformation **g**roper) es una herramienta flexible para realizar consultas en **Servidores DNS**. Realiza búsquedas y muestra las respuestas que son regresadas por los servidores que fueron consultados. Debido a su flexibilidad y claridad en la salida, es que la mayoría de los administradores utilizan **dig** para diagnosticar problemas de DNS.

De modo predeterminado, realiza las búsquedas en los **Servidores DNS** definidos en el archivo **/etc/resolv.conf**, pudiendo definirse de manera opcional cualquier otro **Servidor DNS**. La sintaxis básica sería:

```
dig @servidor dominio.tld TIPO
```

Donde **servidor** corresponde al nombre o dirección IP del **Servidor DNS** a consultar, **dominio.tld** corresponde al nombre del registro del recurso que se está buscando y **TIPO** corresponde al tipo de consulta requerido (ANY, A, MX, SOA, NS, etc.)

Ejemplo:

```
dig @8.8.8.8 alcancelibre.org MX
```

Lo anterior realiza una búsqueda en el **Servidor DNS** en la dirección IP 8.8.8.8 para los registros **MX** para el dominio *alcancelibre.org*.

```
dig alcancelibre.org NS
```

Lo anterior realiza una búsqueda en los **Servidores DNS** definidos en el archivo **/etc/resolv.conf** del sistema para los registros **NS** para el dominio *alcancelibre.org*.

```
dig @8.8.8.8 alcancelibre.org NS
```

Lo anterior realiza una búsqueda en los **Servidor DNS** en la dirección IP 8.8.8.8 para los registros **NS** para el dominio *alcancelibre.org*.

46.2.5.3. Mandato jwhois (whois).

El mandato **jwhois** es una herramienta de consulta a través de servidores **WHOIS**. La sintaxis básica es:

```
jwhois dominio.tld
```

Ejemplo:

```
jwhois alcancelibre.org
```

Lo anterior regresa la información correspondiente al dominio *alcancelibre.org*.

46.3. Modificaciones necesarias en el muro cortafuegos.

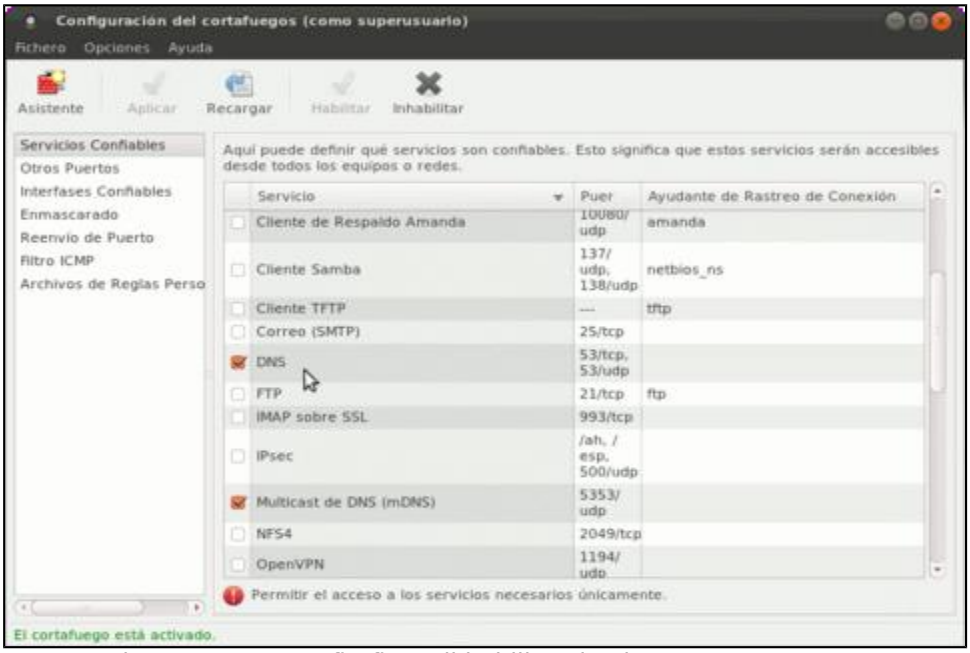
Es necesario abrir en el muro cortafuegos el puerto 53 (dns), tanto por TCP como UDP.

46.3.1. System-config-firewall.

Si utiliza el muro cortafuegos predeterminado del sistema, puede ejecutar el siguiente mandato:

```
system-config-firewall
```

Y habilite DNS y aplique los cambios.



Herramienta system-config-firewall habilitando el puerto 53 por TCP y UDP.

46.3.2. Servicio iptables.

Puede utilizar directamente el mandato **iptables**, ejecutando lo siguiente:

```
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 53 -j ACCEPT
iptables -A INPUT -m state --state NEW -m udp -p udp --dport 53 -j ACCEPT

service iptables save
```

O bien edite el archivo **/etc/sysconfig/iptables**:

```
vim /etc/sysconfig/iptables
```

Y añada el siguiente contenido:

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 53 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 53 -j ACCEPT
```

Para aplicar los cambios, reinicie el servicio **iptables**:

```
service iptables restart
```

46.3.3. Shorewall.

Edite el archivo **/etc/shorewall/rules**:

```
vim /etc/shorewall/rules
```

Las reglas para permitir el acceso al servidor DNS en el anfitrión local corresponderían a algo similar a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  all     fw      tcp     53
ACCEPT  all     fw      udp     53
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Si se desea que los clientes de una red de área local puedan hacer uso de servidores DNS en Internet, es necesario abrir la salida para el puerto 53 (dns), por TCP y UDP.

Las reglas para el archivo **/etc/shorewall/rules** de **Shorewall** correspondería a algo similar a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  all     fw      tcp     53
ACCEPT  all     fw      udp     53
ACCEPT  loc     net     tcp     53
ACCEPT  loc     net     udp     53
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Para aplicar los cambios, reinicie el servicio **shorewall**:

```
service shorewall restart
```

47. Configuración de servidor de nombres de dominio (DNS).

Autor: *Joel Barrios Dueña*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

47.1. Introducción.

Es imprescindible primero estudiar y comprender, los conceptos descritos en el documento titulado «**Introducción al protocolo DNS**.»

47.1.1. Acerca de Bind (Berkeley Internet Name Domain).

BIND (acrónimo de **B**erkeley **I**nternet **N**ame **D**omain) es una implementación del protocolo DNS y provee una implementación libre de los principales componentes del Sistema de Nombres de Dominio, los cuales incluyen:

- Un servidor de sistema de nombres de dominio (named).
- Una biblioteca resolutoria de sistema de nombres de dominio.
- Herramientas para verificar la operación adecuada del servidor DNS (bind-utils).

El Servidor DNS BIND es utilizado de manera amplia en Internet en aproximadamente el 99% de los servidores DNS del mundo, proporcionando una robusta y estable solución.

47.2. Equipamiento lógico necesario.

Paquete.	**Descripción.**
bind	Incluye el **Servidor DNS** (**named**) y herramientas para verificar su funcionamiento.
bind-libs	Bibliotecas compartidas, que consisten en rutinas para aplicaciones para utilizarse cuando se interactúe con **Servidores DNS**.
bind-chroot	Contiene un árbol de archivos que puede ser utilizado como una jaula *chroot* para **named** añadiendo seguridad adicional al servicio.
bind-utils	Colección de herramientas para consultar **Servidores DNS**.
caching-nameserver	Archivos de configuración que harán que el **Servidor DNS** actúe como un caché para el servidor de nombres. Este paquete desaparece en **CentOS 6** y **Red Hat™ Enterprise Linux 6**, pues su contenido se incorporó en el paquete principal de **bind**.

47.2.1. Instalación a través de yum.

Si se utiliza **CentOS 6** o **Red Hat™ Enterprise Linux 6**, se puede instalar **Bind 9.8** utilizando lo siguiente:

```
yum -y install bind bind-chroot bind-utils
```

Si se utiliza **CentOS 5** o **Red Hat™ Enterprise Linux 5** se puede instalar **Bind 9.3.6** utilizando lo siguiente:

```
yum -y install bind bind-chroot bind-utils caching-nameserver
```

Si se utiliza **CentOS 5** o **Red Hat™ Enterprise Linux 5**, también puede instalar, aunque de manera opcional, **Bind 9.7**, el cual incluye soporte para **DNSSEC**, utilizando lo siguiente:

```
yum remove bind-libs bind-utils bind bind-chroot caching-nameserver
yum -y install bind97 bind97-chroot bind97-utils
```

47.2.2. Firma digital del servidor.

Con la finalidad de mejorar la seguridad, genere una firma digital de 512 bits (el valor predeterminado es 128 bits) para el servidor DNS. Ejecute lo siguiente:

```
rndc-confgen -a -r /dev/urandom -b 512 -c /etc/rndc.key
```

Cambie las pertenencias para que este archivo sea propiedad del usuario **root** y grupo **named**:

```
chown root:named /etc/rndc.key
```

Asegure que los permisos de acceso sean lectura y escritura para usuario, sólo lectura para grupo y nada para otros, es decir un permiso 640 (rw-r-----):

```
chmod 640 /etc/rndc.key
```

47.2.3. Actualice el archivo de cache con los servidores DNS raíz.

El archivo **/var/named/named.ca** contiene la información de los servidores DNS raíz necesaria para poder iniciar el cache de todo servidor DNS de Internet. Actualice este archivo para evitar problemas para la resolución de algunas zonas ejecutando lo siguiente:

```
wget -N http://www.internic.net/domain/named.root \
    -O /var/named/named.ca
```

También puede ejecutar lo siguiente para lograr el mismo fin.

```
dig +bufsize=1200 +norec NS . @a.root-servers.net > /var/named/named.ca
```

Conviene verificar periódicamente si hay alguna actualización de este archivo. La versión más reciente al momento de redactar este documento corresponde al 3 de enero de 2013.

El archivo debe pertenecer a **root** y el grupo **named**.

```
chown root:named /var/named/named.ca
```

Asigne permiso de lectura y escritura para usuario, sólo lectura para grupo y nada para otros (rw-r-----).

```
chmod 640 /var/named/named.ca
```

47.3. Procedimientos.

47.3.1. SELinux y el servicio named.

A mediados de 2008, Common Vulnerabilities and Exposures List y US-CERT, reportaron que el investigador **Dan Kaminsky** descubrió una vulnerabilidad que afectaba a varias implementaciones de **DNS** (BIND 8 y 9 antes de 9.5.0-P1, 9.4.2-P1 y 9.3.5-P1; Microsoft DNS en todas las versiones de Windows 2000 SP4, XP SP2 y SP3, así como Server 2003 SP1 y SP2).

Esta vulnerabilidad permite a cualquier atacante remoto el poder falsificar tráfico DNS a través de ciertas técnicas de contaminación de cache en servidores que realizan resolución recursiva (es decir cuando se usa la opción *allow-recursion* abierta a todo el mundo, como ocurre en los servidores DNS públicos) y se relaciona a insuficiente aleatoriedad de las identidades de transacción y de los puertos de origen. Es decir, una vulnerabilidad de entropía de insuficiencia de zócalos (*sockets*) de DNS (conocido como **DNS Insufficient Socket Entropy Vulnerability**). A través de esta vulnerabilidad un atacante puede contaminar el cache de un servidor DNS y hacer que los clientes se conecten hacia direcciones falsas. Es importante aclarar que en realidad se trata de una vulnerabilidad en el diseño del protocolo DNS.

SELinux protege casi por completo al servicio **named** contra la vulnerabilidad anteriormente descrita. Es por tal motivo que es importante utilizar SELinux.

A fin de que SELinux permita al servicio **named** trabajar con permisos de escritura para zonas maestras, es decir un esquema de servidor maestro con servidores esclavos o bien como servidor DNS dinámico, utilice el siguiente mandato:

```
setsebool -P named_write_master_zones 1
```

Lo anterior aplica para **CentOS 5** y **6** y **Red Hat Enterprise Linux 5** y **6**.

Nota.

Sólo para **CentOS 5** y **Red Hat Enterprise Linux 5**: Para definir que se desactive la protección de SELinux para el servicio **named**, haciendo que todo lo anteriormente descrito en esta sección pierda sentido y que el servidor sea parcialmente **susceptible a la vulnerabilidad descubierta por Kaminski**, utilice el siguiente mandato:

```
setsebool -P named_disable_trans 1
```

Sí realiza el procedimiento anterior, es importante configurar la función de consultas recursivas exclusivamente para redes en la que se confíe plenamente.

Esta política, al igual que otras similares, fue eliminada en **CentOS 6** y **Red Hat Enterprise Linux 6**.

Cualquier archivo de zona que se vaya a utilizar a través del servicio **named**, debe contar con los contextos de SELinux de usuario de sistema (**system_u**), rol de objeto (**object_r**) y tipo zona del servicio **named** (**named_zone_t**).

En el siguiente ejemplo se utiliza el mandato **chcon** para cambiar los contextos del archivo denominado **mi-dominio.zone**, con el fin de definir los contextos de SELinux que requiere éste:

```
cd /var/named/data/
chcon -u system_u -r object_r -t named_zone_t mi-dominio.zone
```

Lo anterior solamente es necesario si el archivo **mi-dominio.zone** fue creado fuera del directorio **/var/named/data/** y fue movido hacia este último.

Nota.

Sí se utiliza **CentOS 5** o **Red Hat™ Enterprise Linux 5** y se va a configurar un DNS dinámico, SELinux impedirá crear los archivos ***.jnl** (*journal*, archivos de registro por diario) correspondientes. Las zonas de DNS dinámicas deben ser almacenadas en directorios específicos que solamente contengan zonas dinámicas. Se debe crear el directorio **/var/named/dynamic** para tal fin ,y configurar éste para qué pertenezca al usuario y grupo, **named** y tenga permisos de lectura, escritura y ejecución para el usuario y grupo **named** (770) y tenga los contextos de SELinux de usuario de sistema (**system_u**), rol de objeto (**object_r**) y tipo cache del servicio **named** (**named_cache_t**), con el fin de permitir escritura en este directorio.

```
cd /var/named/
mkdir dynamic/
chmod 770 dynamic/
chown named:named dynamic/
chcon -u system_u -r object_r -t named_cache_t dynamic/
```

Este directorio viene incluido en la instalación estándar de **Bind 9.7** en **CentOS 6** o **Red Hat™ Enterprise Linux 6**, por lo cual es innecesario realizar el procedimiento anterior con estos sistemas operativos.

47.3.2. Configuración mínima para el archivo /etc/named.conf.

Puede descargar un archivo plantilla desde AlcanceLibre.org, ejecutando lo siguiente:

```
cd /etc/
mv named.conf named.conf.original
wget http://www.alcancelibre.org/linux/secrets/named.conf
restorecon named.conf
cd
```

Edite el archivo **/etc/named.conf**:

```
vim /etc/named.conf
```

La configuración mínima de este archivo y la cual permitirá utilizar el servicio para todo tipo de uso, es la siguiente:

```
options {
        directory "/var/named";
        dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        forwarders {
                8.8.8.8;
                8.8.4.4;
        };
        forward first;
// Sólo habilite lo siguiente si va a utilizar DNSSEC y si los servidores de
// la sección de forwarders tienen soporte para DNSSEC.
        dnssec-enable no;
        dnssec-validation no;
//      dnssec-lookaside auto;
//      bindkeys-file "/etc/named.iscdlv.key";
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
        category lame-servers { null; };
};

controls {
        inet 127.0.0.1 allow { 127.0.0.1; } keys { "rndc-key"; };
};

include "/etc/rndc.key";

view "local" {
        match-clients {
                127.0.0.0/8;
                10.0.0.0/8;
                172.16.0.0/12;
                192.168.0.0/16;
        };
        recursion yes;
        include "/etc/named.rfc1912.zones";
        zone "." IN {
                type hint;
                file "named.ca";
        };
};
```

Lo anterior define como opciones que el directorio predeterminado será **/var/named**, se define un archivo donde se almacena la información del caché en **/var/named/data/cache_dump.db**; un archivo de estadísticas en **/var/named/data/named_stats.txt**, un archivo de estadísticas específicas en lo concerniente al uso de la memoria en **/var/named/data/named_mem_stats.txt**; consultas recursivas permitidas solamente a 127.0.0.1 y 192.168.1.0/24, se definen como **ejemplos** de servidores DNS para reenviar consultas a **8.8.8.8** y **8.8.4.4**, que corresponden a los servidores DNS públicos de Google, los cuales puede **reemplazar por los servidores DNS del proveedor de acceso a Internet utilizado**); se define que la primera opción al realizar una consulta será reenviar a los DNS que se acaban de definir; se incluyen los archivos de configuración **/etc/named.rfc1912.zones**, que corresponde a las zonas del **RFC 1912** y la firma digital única que se generó automáticamente tras instalar el paquete bind; Se define que los controles se realizan solamente desde 127.0.0.1, hacia 127.0.0.1, utilizando la firma digital única.

Tome en consideración que los cambios en **CentOS 6** y **Red Hat™ Enterprise Linux 6** respecto de **CentOS 5** y **Red Hat™ Enterprise Linux 5**, consisten en que se utiliza **rndc-key** en lugar de **rndckey** en la configuración de la firma digital, se añaden las líneas correspondientes a la configuración de **DNSSEC**, se añade configuración para el registro en bitácora y la zona de los servidores raíz va separada del archivo **named.rfc1912.zones**. **CentOS 5** y **Red Hat™ Enterprise Linux 5** puede utilizar exactamente la misma configuración instalando los paquetes **bind97**, **bind97-chroot**, **bind97-libs** y **bind97-utils** (desaparece el paquete **caching-nameserver**, cuyo contenido se integró al paquete **bind97**).

Conviene asegurarse que el archivo **/etc/named.conf** tenga los contextos correspondientes para SELinux a fin de evitar potenciales problemas de seguridad.

```
chcon -u system_u -r object_r -t named_conf_t /etc/named.conf
```

47.3.3. Preparativos para añadir dominios.

Idealmente se deben definir primero los siguiente datos:

1. Dominio a resolver.
2. Servidor de nombres principal (SOA). **Éste debe ser un nombre que ya esté plenamente resuelto,** y debe ser un **FQDN** (**F**ully **Q**ualified **D**omain **N**ame).
3. Lista de todos los servidores de nombres (NS) que se utilizarán para efectos de redundancia. **Éstos deben ser nombres que ya estén plenamente resueltos** y deben ser además **FQDN** (**F**ully **Q**ualified **D**omain **N**ame).
4. Cuenta de correo del administrador responsable de esta zona. **Dicha cuenta debe existir y debe ser independiente de la misma zona que se está tratando de resolver.**
5. Al menos un servidor de correo (MX), con un registro **A**, nunca **CNAME**.
6. IP predeterminada del dominio.
7. Sub-dominios dentro del dominio (www, mail, ftp, ns, etc.) y las direcciones IP que estarán asociadas a éstos.

Es importante tener bien en claro que los puntos 2, 3 y 4, involucran datos que **deben existir previamente** y estar plenamente resueltos por otro servidor DNS; Lo anterior quiere decir que jamás se deben utilizar datos que sean parte o dependan, del mismo dominio que se pretende resolver. De igual modo, el servidor donde se implementará el **DNS** deberá contar con un nombre **FQDN** y que esté previa y plenamente, resuelto en otro DNS.

Como regla general, se generará una zona de reenvío por cada dominio sobre el cual se tenga autoridad plena y absoluta y se generará una zona de resolución inversa por cada red sobre la cual se tenga plena y absoluta autoridad. Es decir, si se es el propietario del dominio *«cualquiercosa.com»*, se deberá generar el archivo de zona correspondiente, con el fin de resolver dicho dominio. Por cada red con direcciones IP privadas, sobre la cual se tenga control y absoluta autoridad, se deberá generar un archivo de zona de resolución inversa a fin de resolver inversamente las direcciones IP de dicha zona.

Regularmente la resolución inversa de las direcciones IP públicas es responsabilidad de los proveedores de servicio ya que son éstos quienes tienen la autoridad plena y absoluta sobre dichas direcciones IP.

Todos los archivos de zona deben pertenecer al usuario «named» a fin de que el servicio **named** pueda acceder a éstos o bien modificar éstos en el caso de tratarse de zonas esclavas.

47.3.4. Creación de los archivos de zona.

Los siguientes corresponderían a los contenidos para los archivos de zona requeridos para la red local y por el NIC con el que se haya registrado el dominio. Cabe señalar que en las zonas de reenvío siempre se especifica al menos un registro **SOA** y un registro **NS**. De manera opcional y en caso de que exista un servicio de correo electrónico, añada al menos un registro **MX** (Mail Exchanger o intercambiador de correo). Solamente necesitará sustituir nombres y direcciones IP y quizá añadir nuevos registros para complementar su red local.

47.3.4.1. Configuración mínima para /etc/named.conf en CentOS 5 y Red Hat™ Enterprise Linux 5.

La configuración mínima del archivo **/chroot/etc/named.conf** y que permitirá utilizar el servicio para todo tipo de uso, es la siguiente:

```
options {
        directory "/var/named";
        dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        forwarders {
                8.8.8.8;
                8.8.4.4;
        };
        forward first;
// Sólo habilite lo siguiente si va a utilizar DNSSEC y si los servidores de
// la sección de forwarders tienen soporte para DNSSEC.
        dnssec-enable no;
        dnssec-validation no;
//      dnssec-lookaside auto;
//      bindkeys-file "/etc/named.iscdlv.key";
};

include "/etc/rndc.key";

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
        category lame-servers { null; };
};

controls {
        inet 127.0.0.1 allow { 127.0.0.1; } keys { "rndckey"; };
};

view "local" {
        match-clients {
                127.0.0.0/8;
                10.0.0.0/8;
                172.16.0.0/12;
                192.168.0.0/16;
        };
        recursion yes;
        include "/etc/named.rfc1912.zones";
};
```

Lo anterior define como opciones que el directorio predeterminado será **/var/named**, se define un archivo donde se almacena la información del caché en **/var/named/data/cache_dump.db**; un archivo de estadísticas en **/var/named/data/named_stats.txt**, un archivo de estadísticas específicas en lo concerniente al uso de la memoria en **/var/named/data/named_mem_stats.txt**; consultas recursivas permitidas solamente a 127.0.0.1 y 192.168.1.0/24; se definen como **ejemplos** de servidores DNS para reenviar consultas a **8.8.8.8** y **8.8.4.4**, que corresponden a servidores DNS públicos de Google, los cuales puede **reemplazar por los servidores DNS del proveedor de acceso a Internet utilizado**; se define que la primera opción al realizar una consulta será reenviar a los DNS que se acaban de definir; se incluyen los archivos de configuración **/etc/named.rfc1912.zones**, que corresponde a las zonas del **RFC 1912** y la firma digital única que se generó automáticamente tras instalar el paquete bind; Se define también que los controles se realizan solamente desde 127.0.0.1, hacia 127.0.0.1, utilizando la firma digital única.

Conviene asegurarse que el archivo **/etc/named.conf** tenga los contextos correspondientes para SELinux a fin de evitar potenciales problemas de seguridad.

```
chcon -u system_u -r object_r -t named_conf_t /etc/named.conf
```

47.3.4.2. Ejemplo de Zona de reenvío red local /var/named/data/red-local.zone.

```
$TTL 86400
@               IN      SOA     dns.red-local.  alguien.gmail.com. (
                2009091001; número de serie
                28800 ; tiempo de refresco
                7200 ; tiempo entre reintentos de consulta
                604800 ; tiempo tras el cual expira la zona
                86400 ; tiempo total de vida
                )
@               IN      NS      dns.red-local.net.
@               IN      MX      10      mail
@               IN      TXT     "v=spf1 a mx -all"
@               IN      A       192.168.1.1
intranet        IN      A       192.168.1.1
maquina2        IN      A       192.168.1.2
maquina3        IN      A       192.168.1.3
maquina4        IN      A       192.168.1.4
www             IN      A       192.168.1.1
mail            IN      A       192.168.1.1
ftp             IN      CNAME   intranet
dns             IN      CNAME   intranet
```

47.3.4.3. Zona de resolución inversa red local /var/named/data/1.168.192.in-addr.arpa.zone

```
$TTL 86400
@               IN      SOA     dns.red-local.  alguien.gmail.com. (
                2009091001 ; número de serie
                28800 ; tiempo de refresco
                7200 ; tiempo entre reintentos de consulta
                604800 ; tiempo tras el cual expira la zona
                86400 ; tiempo total de vida
                )
@               IN      NS      dns.red-local.
1       IN      PTR     intranet.red-local.
2       IN      PTR     maquina2.red-local.
3       IN      PTR     maquina3.red-local.
4       IN      PTR     maquina4.red-local.
```

47.3.4.4. Zona de reenvío del dominio /var/named/data/dominio.com.zone

Suponiendo que hipotéticamente se es la autoridad para el dominio **«dominio.com»**, se puede crear una **Zona de Reenvío** con un contenido similar al siguiente:

```
$TTL 86400
@               IN      SOA     fqdn.dominio.tld.       alguien.gmail.com. (
                2009091001; número de serie
                28800 ; tiempo de refresco
                7200 ; tiempo entre reintentos de consulta
                604800 ; tiempo tras el cual expira la zona
                86400 ; tiempo total de vida
                )
@               IN      NS      fqdn.dominio.tld.
@               IN      MX      10      mail
@               IN      TXT     "v=spf1 a mx -all"
@               IN      A       201.161.1.226
servidor        IN      A       201.161.1.226
www             IN      A       201.161.1.226
mail            IN      A       201.161.1.226
ftp             IN      CNAME   servidor
dns             IN      CNAME   servidor
```

47.3.4.5. Zona de resolución inversa del dominio /var/named/data/1.161.201.in-addr.arpa.zone

Suponiendo que hipotéticamente se es la autoridad para el segmento de red **201.161.1.0/24** (regularmente lo debe de hacer el proveedor de servicio de acceso hacia Internet), se puede crear una **Zona de Resolución Inversa** con un contenido similar al siguiente:

```
$TTL 86400
@               IN      SOA     fqdn.dominio.tld.       alguien.gmail.com. (
                2009091001 ; número de serie
                28800 ; tiempo de refresco
                7200 ; tiempo entre reintentos de consulta
                604800 ; tiempo tras el cual expira la zona
                86400 ; tiempo total de vida
                )
@               IN      NS      fqdn.dominio.tld.
1       IN      PTR     servidor.dominio.com.
2       IN      PTR     maquina2.dominio.com.
3       IN      PTR     maquina3.dominio.com.
4       IN      PTR     maquina4.dominio.com.
```

Cada vez que haga algún cambio en algún archivo de zona, deberá cambiar el número de serie a fin de que tomen efecto los cambios de inmediato cuando se reinicie el servicio **named**, ya que de otro modo tendría que reiniciar el equipo, algo poco conveniente.

Las zonas de resolución inversa que involucran direcciones IP públicas son responsabilidad de los ISP (proveedores de servicio de acceso hacia Internet). Crear una zona de resolución inversa sin ser la autoridad de dicha zona tiene efecto sólo para quien use el servidor DNS recién configurado como único DNS.

47.3.4.6. Configuración de parámetros en el archivo /etc/named.conf

```
options {
        directory "/var/named";
        dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        forwarders {
                8.8.8.8;
                8.8.4.4;
        };
        forward first;
// Sólo habilite lo siguiente si va a utilizar DNSSEC y si los servidores de
// la sección de forwarders tienen soporte para DNSSEC.
        dnssec-enable no;
        dnssec-validation no;
//      dnssec-lookaside auto;
//      bindkeys-file "/etc/named.iscdlv.key";
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
        category lame-servers { null; };
};

controls {
        inet 127.0.0.1 allow { 127.0.0.1; } keys { "rndc-key"; };
};

include "/etc/rndc.key";

view "local" {
        match-clients {
                127.0.0.0/8;
                10.0.0.0/8;
                172.16.0.0/12;
                192.168.0.0/16;
        };
        recursion yes;
        include "/etc/named.rfc1912.zones";
        zone "." IN {
                type hint;
                file "named.ca";
        };
        zone "red-local" {
                type master;
                file "data/red-local.zone";
                allow-update { none; };
        };
        zone "1.168.192.in-addr.arpa" {
                type master;
                file "data/1.168.192.in-addr.arpa.zone";
                allow-update { none; };
        };
};
```

47.3.5. Seguridad adicional en DNS para uso público.

Quienes hayan utilizado en recientes fechas los servicios de DNS Report, habrán notado que el diagnóstico en línea devuelve ahora un error que, en resumen, indica que el servidor puede ser susceptible de sufrir/participar en un ataque **DDoS** (**D**istributed **D**enail **o**f **S**ervice o denegación de servicio distribuido).

Un **DDoS** (**D**istributed **D**enial **o**f **S**ervice) es una ampliación del ataque **DoS**, se efectúa con la instalación de varios agentes remotos en muchas computadoras que pueden estar localizadas en diferentes puntos del mundo. El atacante consigue coordinar esos agentes para así, de forma masiva, amplificar el volumen del saturación de información (*flood*), pudiendo darse casos de un ataque de cientos o millares de computadoras dirigido a una máquina o red objetivo. Esta técnica se ha revelado como una de las más eficaces y sencillas a la hora de colapsar servidores, la tecnología distribuida ha ido haciendo más sofisticada hasta el punto de otorgar poder de causar daños serios a personas con escaso conocimiento técnico.

La falla reportada por la herramienta en línea de DNS Report, para un servidor DNS que permite consultas recursivas, indicará algo como lo siguiente:

> *«ERROR: One or more of your nameservers reports that it is an open DNS server. This usually means that anyone in the world can query it for domains it is not authoritative for (it is possible that the DNS server advertises that it does recursive lookups when it does not, but that shouldn't happen). This can cause an excessive load on your DNS server. Alos, it is strongly discouraged to have a DNS server be both authoritative for your domain and be recursive (even if it is not open), due to the potential for cache poisoning (with no recursion, there is no cache, and it is impossible to poison it). Alos, the bad guys could use your DNS server as part of an attack, by forging their IP address»*

Significa que el servidor DNS puede permitir a cualquiera realizar consultas recursivas. Si se trata de un DNS que se desea pueda ser consultado por cualquiera, como puede ser el caso del DNS de un ISP, esto es normal y esperado. Si se trata de un servidor que sólo debe consultar la red local o bien que se utiliza para propagar dominios alojados de manera local, si es conveniente tomar medidas al respecto.

Solución al problema es modificar el archivo **named.conf**, donde se añade en la sección de vista local (view "local") la opción **recursion yes;** y una o más líneas que definan a la red o las redes que tendrán permitido realizar todo tipo de consultas.

```
options {
        directory "/var/named";
        dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        forwarders {192.168.0.1; };
        forward first;
        dnssec-enable yes;
        dnssec-validation yes;
        dnssec-lookaside auto;
        bindkeys-file "/etc/named.iscdlv.key";
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

controls {
        inet 127.0.0.1 allow { 127.0.0.1; } keys { "rndc-key"; };
};

include "/etc/rndc.key";

view "local" {
        match-clients {
                127.0.0.0/8;
                10.0.0.0/8;
                172.16.0.0/12;
                192.168.0.0/16;
        };
        recursion yes;
        include "/etc/named.rfc1912.zones";
        zone "." IN {
                type hint;
                file "named.ca";
        };
};
```

Lo anterior hace que sólo se puedan realizar consultas recursivas en el DNS desde 127.0.0.0/8, 10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16, ya sea para un nombre de dominio alojado de manera local y otros dominios resueltos en otros servidores (ejemplo: www.yahoo.com, www.google.com, www.alcancelibre.org, etc). El resto del mundo sólo podrá realizar consultas sobre los dominios alojados de manera local y que estén configurado para permitirlo.

En la siguiente configuración de ejemplo, se pretende lograr lo siguiente:

- Red Local: cualquier tipo de consulta hacia dominios externos y locales (es decir, www.yahoo.com, www.google.com, alcancelibre.org, además de ***midominio.com***).
- Resto del mundo: sólo puede hacer consultas para la zona de ***midominio.com***

De este modo se impide que haya consultas recursivas y con esto impedir la posibilidad de sufrir/participar de un ataque DDoS.

```
options {
        directory "/var/named";
        dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        forwarders {192.168.0.1; };
        forward first;
        dnssec-enable yes;
        dnssec-validation yes;
        dnssec-lookaside auto;
        bindkeys-file "/etc/named.iscdlv.key";
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

controls {
        inet 127.0.0.1 allow { 127.0.0.1; } keys { "rndc-key"; };
};

include "/etc/rndc.key";

view "publico" {
        match-clients { any; };
        recursion no;
        zone "." IN {
                type hint;
                file "named.ca";
        };
        zone "midominio.com" {
                type master;
                file "data/midominio.com.zone";
                allow-update { none; };
                allow-transfer { 200.76.185.252; 200.76.185.251; };
        };
};

view "local" {
        match-clients {
                127.0.0.0/8;
                10.0.0.0/8;
                172.16.0.0/12;
                192.168.0.0/16;
        };
        recursion yes;
        include "/etc/named.rfc1912.zones";
        zone "." IN {
                type hint;
                file "named.ca";
        };
        zone "miredlocal" {
                type master;
                file "data/miredlocal.zone";
                allow-update { none; };
                allow-transfer { 192.168.0.2; };
        };
};
```

Un **DDoS** (**D**istributed **D**enial **o**f **S**ervice) es una ampliación del ataque **DoS**, se efectúa con la instalación de varios agentes remotos en muchas computadoras que pueden estar localizadas en diferentes puntos del mundo. El atacante consigue coordinar esos agentes para así, de forma masiva, amplificar el volumen del saturación de información (flood), pudiendo darse casos de un ataque de cientos o millares de computadoras dirigido a una máquina o red objetivo. Esta técnica se ha revelado como una de las más eficaces y sencillas a la hora de colapsar servidores, la tecnología distribuida ha ido haciendo más sofisticada hasta el punto de otorgar poder de causar daños serios a personas con escaso conocimiento técnico.

La falla reportada por la herramienta en línea de DNS Report, para un servidor DNS que permite consultas recursivas, indicará algo como lo siguiente:

> *«ERROR: One or more of your nameservers reports that it is an open DNS server. This usually means that anyone in the world can query it for domains it is not authoritative for (it is possible that the DNS server advertises that it does recursive lookups when it does not, but that shouldn't happen). This can cause an excessive load on your DNS server. Alos, it is strongly discouraged to have a DNS server be both authoritative for your domain and be recursive (even if it is not open), due to the potential for cache poisoning (with no recursion, there is no cache, and it is impossible to poison it). Alos, the bad guys could use your DNS server as part of an attack, by forging their IP address»*

Significa que el servidor DNS puede permitir a cualquiera realizar consultas recursivas. Si se trata de un DNS que se desea pueda ser consultado por cualquiera, como puede ser el caso del DNS de un ISP, esto es normal y esperado. Si se trata de un servidor que sólo debe consultar la red local o bien que se utiliza para propagar dominios alojados de manera local, si es conveniente tomar medidas al respecto.

Solución al problema es modificar el archivo **named.conf**, donde se añade en la sección de vista local (view "local") la opción **recursion yes;** y una o más líneas que definan la red o las redes que tendrán permitido realizar todo tipo de consultas.

```
options {
        directory "/var/named";
        dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        forwarders { 192.168.70.1; };
        forward first;
        dnssec-enable yes;
        dnssec-validation yes;
        dnssec-lookaside auto;
        bindkeys-file "/etc/named.iscdlv.key";
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

controls {
        inet 127.0.0.1 allow { 127.0.0.1; } keys { "rndc-key"; };
};

include "/etc/rndc.key";

view "local" {
        match-clients {
                127.0.0.0/8;
                10.0.0.0/8;
                172.16.0.0/12;
                192.168.0.0/16;
        };
        recursion yes;
        include "/etc/named.rfc1912.zones";
        zone "." IN {
                type hint;
                file "named.ca";
        };
};
```

Lo anterior hace que sólo se puedan realizar todo tipo de consultas en el DNS desde 127.0.0.0/8, 10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16, ya sea para un nombre de dominio alojado de manera local y otros dominios resueltos en otros servidores (ejemplo: *www.yahoo.com*, *www.google.com*, *www.alcancelibre.org*, etc). El resto del mundo sólo podrá realizar consultas sobre los dominios alojados de maneja local y que estén configurado para permitirlo.

En la siguiente configuración de ejemplo, se pretende lograr lo siguiente:

- Red Local: cualquier tipo de consulta hacia dominios externos y locales (es decir, www.yahoo.com, www.google.com, alcancelibre.org, además de ***midominio.com***).

- Resto del mundo: sólo puede hacer consultas para la zona de ***midominio.com***

De este modo se impide que haya consultas recursivas y con esto impedir la posibilidad de sufrir/participar de un ataque DDoS.

```
options {
        directory "/var/named";
        dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        forwarders {192.168.0.1; };
        forward first;
        dnssec-enable yes;
        dnssec-validation yes;
        dnssec-lookaside auto;
        bindkeys-file "/etc/named.iscdlv.key";

};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

controls {
        inet 127.0.0.1 allow { 127.0.0.1; } keys { "rndc-key"; };
};

include "/etc/rndc.key";

view "publico" {
        match-clients { any; };
        recursion no;
        zone "." IN {
                type hint;
                file "named.ca";
        };
        zone "midominio.com" {
               type master;
              file "data/midominio.com.zone";
              allow-update { none; };
             allow-transfer { 204.13.249.75; 208.78.69.75; 91.198.22.75; };
        };
};

view "local" {
        match-clients {
                127.0.0.0/8;
                10.0.0.0/8;
                172.16.0.0/12;
                192.168.0.0/16;
        };
        recursion yes;
        include "/etc/named.rfc1912.zones";
        zone "." IN {
                type hint;
                file "named.ca";
        };
        zone "miredlocal" {
               type master;
               file "data/miredlocal.zone";
               allow-update { none; };
               allow-transfer { 192.168.0.2; };
        };
};
```

47.3.6. Seguridad adicional en DNS para uso exclusivo en red local.

Si se va a tratar de un servidor de nombres de dominio para uso exclusivo en red local y se quieren evitar problemas de seguridad de diferente índole, puede utilizarse el parámetro **allow-query**, el cual servirá para especificar que sólo ciertas direcciones podrán realizar consultas al servidor de nombres de dominio. Se pueden especificar directamente direcciones IP, redes completas o listas de control de acceso que deberán definirse antes de cualquier otra cosa en el archivo **/etc/named.conf**.

47.3.6.1. Archivo /etc/named.conf

```
options {
        directory "/var/named/";
        dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        forwarders {
                8.8.8.8;
                8.8.4.4;
        };
        forward first;
        dnssec-enable yes;
        dnssec-validation yes;
        dnssec-lookaside auto;
        bindkeys-file "/etc/named.iscdlv.key";
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

controls {
        inet 127.0.0.1 allow { 127.0.0.1; } keys { "rndc-key"; };
};

include "/etc/rndc.key";

view "local" {
        match-clients {
                127.0.0.0/8;
                10.0.0.0/8;
                172.16.0.0/12;
                192.168.0.0/16;
        };
        recursion yes;
        include "/etc/named.rfc1912.zones";
        zone "." IN {
                type hint;
                file "named.ca";
        };
        zone "red-local" {
                type master;
                file "data/red-local.zone";
                allow-update { none; };
        };
        zone "1.168.192.in-addr.arpa" {
                type master;
                file "data/1.168.192.in-addr.arpa.zone";
                allow-update { none; };
        };
};
```

47.3.7. Las zonas esclavas.

Las zonas esclavas se refieren a aquellas hospedadas en servidores de nombres de dominio secundarios y que hacen las funciones de redundar las zonas maestras en los servidores de nombres de dominio primarios. El contenido del archivo de zona es el mismo que en servidor primario. La diferencia está en la sección de texto utilizada en **named.conf**, donde las zonas se definen como esclavas y definen los servidores donde está hospedada la zona maestra.

47.3.7.1. Archivo named.conf Servidor DNS secundario.

```
view "publico" {
        match-clients { any; };
        recursion no;
        zone "." IN {
                type hint;
                file "named.ca";
        };
        zone "dominio.com" {
                type slave;
                file "dominio.com.zone";
                masters { 192.168.1.254; };
        };
};

view "local" {
        match-clients {
                127.0.0.0/8;
                10.0.0.0/8;
                172.16.0.0/12;
                192.168.0.0/16;
        };
        recursion yes;
        include "/etc/named.rfc1912.zones";
        zone "." IN {
                type hint;
                file "named.ca";
        };
        zone "red-local" {
                type slave;
                file "data/red-local.zone";
                masters { 192.168.1.254; };
        };
        zone "1.168.192.in-addr.arpa" {
                type slave;
                file "data/1.168.192.in-addr.arpa.zone";
                masters { 192.168.1.254; };
        };
};
```

Adicionalmente, si desea incrementar seguridad y desea especificar **en el Servidor DNS Primario** que servidores tendrán permitido ser servidores de nombres de dominio secundario, es decir, hacer transferencias, puede utilizar el parámetro **allow-transfer** del siguiente modo:

47.3.7.2. Archivo named.conf Servidor DNS Primario.

```
view "publico" {
        match-clients { any; };
        recursion no;
        zone "." IN {
                type hint;
                file "named.ca";
        };
        zone "dominio.com" {
                type master;
                file "dominio.com.zone";
                allow-update { none; };
                allow-transfer {
                        200.33.146.217;
                        200.33.146.209;
                };
        };
};

view "local" {
        match-clients {
                127.0.0.0/8;
                10.0.0.0/8;
                172.16.0.0/12;
                192.168.0.0/16;
        };
        recursion yes;
        include "/etc/named.rfc1912.zones";
        zone "." IN {
                type hint;
                file "named.ca";
        };
        zone "red-local" {
                type master;
                file "data/red-local.zone";
                allow-update { none; };
                allow-transfer {
                        192.168.1.15;
                        192.168.1.16;
                };
        };
        zone "1.168.192.in-addr.arpa" {
                type master;
                file "data/1.168.192.in-addr.arpa.zone";
                allow-update { none; };
                allow-transfer {
                        192.168.1.15;
                        192.168.1.16;
                };
        };
};
```

47.3.8. Seguridad adicional para transferencias de zona.

Cuando se gestionan dominios a través de redes públicas, es importante considerar que si se tienen esquemas de servidores **maestros** y **esclavos**, siempre será más conveniente utilizar una **clave cifrada** en lugar de una dirección IP, debido a que esta última puede ser falsificada bajo ciertas circunstancias.

Comúnmente se definen las direcciones IP desde las cuales se permitirá transferencias de zonas, utilizando una configuración en el archivo **/etc/named.conf** como la ejemplificada a continuación, donde los servidores esclavos corresponden a los servidores con direcciones IP 192.168.1.11 y 192.168.1.12:

```
zone "mi-dominio.org" {
        type master;
        file "data/mi-dominio.org.zone";
        allow-update { none; }:
        allow-transfer { 192.168.1.11; 192.168.1.12; };
};
```

Lo anterior permite la transferencia de zona para los servidores con direcciones IP 192.168.1.11 y 192.168.1.12, los cuales utilizan la siguiente configuración en el archivo **/etc/named.conf**, ejemplificada a continuación, donde el servidor primario (zonas maestras) corresponde al servidor con dirección IP 192.168.1.1:

```
zone "mi-dominio.org" {
        type slave;
        file "data/mi-dominio.org.zone";
        masters { 192.168.1.1; };
};
```

El inconveniente del esquema anterior es que es fácil falsificar las direcciones IP. A fin de evitar que esto ocurra, el método recomendado será utilizar una clave cifrada que será validada en lugar de la dirección IP. La llave se crea con el mandato **dnssec-keygen**, especificando un algoritmo, que puede ser **RSAMD5** o **RSA**, **DSA**, **DH** (**D**iffie **H**ellman) o **HMAC-MD5**, el tamaño de la llave en octetos (bits), el tipo de la llave, que puede ser ZONE, HOST, ENTITY o USER y el nombre específico para la clave cifrada. DSA y RSA se utilizan para **DNS Seguro** (**DNSSEC**), en tanto que **HMAC-MD5** se utiliza para **TSIG** (**T**ransfer **SIG**nature o transferencia de firma). Lo más común es utilizar **TSIG**. En el siguiente ejemplo, se generará en el directorio de trabajo actual la clave **mi-dominio.org**, utilizando **/dev/random** como fuente de datos aleatorios, un algoritmo **HMAC-MD5** tipo **HOST** de 128 octetos (bits):

```
dnssec-keygen -r /dev/random -a HMAC-MD5 -b 128 -n HOST mi-dominio.org
```

Lo anterior devuelve una salida similar a la siguiente:

```
Kmi-dominio.org.+157+32322
```

Al mismo tiempo se generaran dos archivos en el directorio **/var/named/**, que corresponderían a **Kmi-dominio.org.+157+32322.key** y **Kmi-dominio.org.+157+32322.private**. **Kmi-dominio.org.+157+32322.key** deberá tener un contenido como el siguiente, el cual corresponde al registro que se añade dentro del archivo de zona:

```
mi-dominio.org. IN KEY 512 3 157 NPuNuxvZAjtd3mriuygT8Q==
```

Kmi-dominio.org.+157+32322.private deberá tener un contenido como el siguiente:

```
Private-key-format: v1.2
Algorithm: 157 (HMAC_MD5)
Key: NPuNuxvZAjtd3mriuygT8Q==
```

En ambos casos, **NPuNuxvZAjtd3mriuygT8Q==** corresponde a la clave cifrada. Ambos deben tener la misma clave.

Los dos archivos sólo deben tener atributos de lectura para el usuario **named**.

```
chmod 400 Kmi-dominio.org.+157+32322.*
chown named.named Kmi-dominio.org.+157+32322.*
```

A fin de poder ser utilizados, ambos archivos deben ser movidos hacia el directorio **/var/named/data/**.

```
mv Kmi-dominio.org.+157+32322.*/var/named/data/
```

A continuación, restaure los atributos predeterminados para estos archivos utilizando el mandato **restorecon**, del siguiente modo:

```
restorecon -R /var/named/data/
```

En el servidor primario (zonas maestras), se añade la siguiente configuración en el archivo **/etc/named.conf**:

```
key mi-dominio.org {
    algorithm HMAC-MD5;
    secret "NPuNuxvZAjtd3mriuygT8Q==";
};

zone "mi-dominio.org" {
        type master;
        file "data/mi-dominio.org.zone";
        allow-update { none; };
        allow-transfer { key mi-dominio.org; };
};
```

Los servidores esclavos utilizarían la siguiente configuración en el archivo **/etc/named.conf**, en donde se define la clave y que ésta será utilizada para realizar conexiones hacia el servidor primario (zonas maestras) (192.168.1.1, en el ejemplo):

```
key mi-dominio.org {
        algorithm HMAC-MD5;
        secret "NPuNuxvZAjtd3mriuygT8Q==";
};

server 192.168.1.1 {
        keys { mi-dominio.org; };
};

zone "mi-dominio.org" {
        type slave;
        masters { 192.168.1.1; };
};
```

47.3.8.1. Comprobaciones.

Tanto en el servidor primario (zonas maestras) como en los servidores esclavos, utilice el mandato **tail** para ver la salida del archivo **/var/log/messages**, pero sólo aquello que contenga la cadena de caracteres **named**:

```
tail -f /var/log/messages |grep named
```

Al reiniciar el servicio **named** en servidor primario (zonas maestras), se debe mostrar una salida similar a la siguiente cuando un servidor esclavo realiza una transferencia:

```
Sep 10 01:57:40 servidor named[6042]: listening on IPv4 interface eth0, 192.168.1.64#53
Sep 10 01:57:40 servidor named[6042]: command channel listening on 127.0.0.1#953
Sep 10 01:57:40 servidor named[6042]: zone 0.in-addr.arpa/IN: loaded serial 42
Sep 10 01:57:40 servidor named[6042]: zone 0.0.127.in-addr.arpa/IN: loaded serial 1997022700
Sep 10 01:57:40 servidor named[6042]: zone 255.in-addr.arpa/IN: loaded serial 42
Sep 10 01:57:40 servidor named[6042]: zone
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa/IN: loaded serial 1997022700
Sep 10 01:57:40 servidor named[6042]: zone localdomain/IN: loaded serial 42
Sep 10 01:57:40 servidor named[6042]: zone localhost/IN: loaded serial 42
Sep 10 01:57:40 servidor named[6042]: zone mi-dominio.org/IN: loaded serial 2009091001
Sep 10 01:57:40 servidor named: Iniciación de named succeeded
Sep 10 01:57:40 servidor named[6042]: running
Sep 10 01:57:40 servidor named[6042]: zone mi-dominio.org/IN: sending notifies (serial 2009091001)
Sep 10 01:59:49 servidor named[6042]: client 192.168.1.11#32817: transfer of 'mi-dominio.org/IN': AXFR
started
```

Al reiniciar el servicio **named** en los servidores esclavos, se debe mostrar una salida similar a la siguiente:

```
Sep 10 01:58:15 servidor named[5080]: listening on IPv4 interface eth0, 192.168.1.253#53
Sep 10 01:58:15 servidor named[5080]: command channel listening on 127.0.0.1#953
Sep 10 01:58:15 servidor named[5080]: zone 0.in-addr.arpa/IN: loaded serial 42
Sep 10 01:58:15 servidor named[5080]: zone 0.0.127.in-addr.arpa/IN: loaded serial 1997022700
Sep 10 01:58:15 servidor named[5080]: zone 255.in-addr.arpa/IN: loaded serial 42
Sep 10 01:58:15 servidor named[5080]: zone
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa/IN: loaded serial 1997022700
Sep 10 01:58:15 servidor named[5080]: zone localdomain/IN: loaded serial 42
Sep 10 01:58:15 servidor named[5080]: zone localhost/IN: loaded serial 42
Sep 10 01:58:15 servidor named[5080]: running
Sep 10 01:58:15 servidor named: Iniciación de named succeeded
Sep 10 01:58:15 servidor named[5080]: zone mi-dominio.org/IN: transferred serial 2009091001
Sep 10 01:58:15 servidor named[5080]: transfer of 'mi-dominio.org/IN' from 192.168.1.1#53: end of
transfer
Sep 10 01:58:15 servidor named[5080]: zone mi-dominio.org/IN: sending notifies (serial 2009091001)
```

47.3.9. Reiniciar servicio y depuración de configuración.

Al terminar de editar todos los archivos involucrados, sólo bastará reiniciar el servidor de nombres de dominio.

```
service named restart
```

Si queremos que el servidor de nombres de dominio quede añadido entre los servicios en el arranque del sistema, deberemos realizar lo siguiente a fin de habilitar **named** junto con el arranque del sistema:

```
chkconfig named on
```

Realice prueba de depuración y verifique que la zona haya cargado con número de serie:

```
tail -80 /var/log/messages |grep named
```

Lo anterior, si está funcionando correctamente, debería devolver algo parecido a lo mostrado a continuación:

```
Sep 10 02:15:15 servidor named[30618]: starting BIND 9.2.2 -u named
Sep 10 02:15:15 servidor named[30618]: using 1 CPU
Sep 10 02:15:15 servidor named: Iniciación de named succeeded
Sep 10 02:15:15 servidor named[30622]: loading configuration from '/etc/named.conf'
Sep 10 02:15:15 servidor named[30622]: no IPv6 interfaces found
Sep 10 02:15:15 servidor named[30622]: listening on IPv4 interface lo, 127.0.0.1#53
Sep 10 02:15:15 servidor named[30622]: listening on IPv4 interface eth0, 192.168.1.1#53
Sep 10 02:15:15 servidor named[30622]: command channel listening on 127.0.0.1#953
Sep 10 02:15:16 servidor named[30622]: zone 0.0.127.in-addr.arpa/IN: loaded serial 3
Sep 10 02:15:16 servidor named[30622]: zone 1.168.192.in-addr.arpa/IN: loaded serial 2009091001
Sep 10 02:15:16 servidor named[30622]: zone localhost/IN: loaded serial 1
Sep 10 02:15:16 servidor named[30622]: zone mi-dominio.com.mx/IN: loaded serial 2009091001
Sep 10 02:15:16 servidor named[30622]: running
Sep 10 02:15:16 servidor named[30622]: zone 1.168.192.in-addr.arpa/IN: sending notifies (serial
2009091001)
Sep 10 02:15:16 servidor named[30622]: zone mi-dominio.com.mx/IN: sending notifies (serial 2009091001)
```

48. Configuración de servidor DHCP.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

48.1. Introducción.

48.1.1. Acerca del protocolo DHCP.

DHCP (acrónimo de ***D****ynamic Host* ***C****onfiguration* ***P****rotocol*, que se traduce Protocolo de configuración dinámica de servidores) es un protocolo que permite a dispositivos individuales en una red de direcciones IP obtener su propia información de configuración de red (dirección IP; máscara de sub-red, puerta de enlace, etc.) a partir de un servidor DHCP. Su propósito principal es hacer más fáciles de administrar las redes grandes. **DHCP** existe desde 1993 como protocolo estándar y se describe a detalle en el RFC 2131.

Sin la ayuda de un servidor **DHCP**, tendrían que configurarse de forma manual cada dirección IP de cada anfitrión que pertenezca a una Red de Área Local. Si un anfitrión se traslada hacia otra ubicación donde existe otra Red de Área Local, se tendrá que configurar otra dirección IP diferente para poder unirse a esta nueva Red de Área Local. Un servidor **DHCP** entonces supervisa y distribuye, las direcciones IP de una Red de Área Local asignando una dirección IP a cada anfitrión que se una a la Red de Área Local. Cuando, por mencionar un ejemplo, una computadora portátil se configura para utilizar **DHCP**, a ésta le será asignada una dirección IP y otros parámetros de red, necesarios para unirse a cada Red de Área Local donde se localice.

Existen tres métodos de asignación en el protocolo **DHCP**:

- **Asignación manual**: La asignación utiliza una tabla con direcciones **MAC** (acrónimo de ***M****edia* ***A****ccess* ***C****ontrol* ***A****ddress*, que se traduce como dirección de Control de Acceso al Medio). Sólo los anfitriones con una dirección **MAC** definida en dicha tabla recibirá el IP asignada en la misma tabla. Ésto se hace a través del parámetro **hardware ethernet** combinado con **deny unknown-clients**.
- **Asignación automática**: Una dirección de IP disponible dentro de un rango determinado se asigna permanentemente al anfitrión que la requiera.
- **Asignación dinámica**: Se determina arbitrariamente un rango de direcciones IP y cada anfitrión conectado a la red está configurada para solicitar su dirección IP al servidor cuando se inicia el dispositivo de red, **utilizando un intervalo de tiempo controlable** (parámetros **default-lease-time** y **max-lease-time**), de modo que la asignación de direcciones IP es de manera temporal y éstas se reutilizan de forma dinámica.

URL: http://www.ietf.org/rfc/rfc2131.txt y http://www.ietf.org/rfc/rfc2132.txt

48.1.2. Acerca de dhcp por Internet Software Consortium, Inc.

Fundado en 1994, Internet Software Consortium, Inc., distribuye un conjunto de herramientas para el protocolo **DHCP**, las cuales consisten en:

- **Servidor DHCP.**
- **Cliente DHCP.**
- **Agente de retransmisión.**

Dichas herramientas utilizan un **API** (**A**pplication **P**rogramming **I**nterface o Interfaz de Programación de Aplicaciones) modular diseñado para ser lo suficientemente general para ser utilizado con facilidad en los sistemas operativos que cumplen el estándar **POSIX** (***P****ortable* ***O****perating* ***S****ystem* ***I****nterface for UNI****X*** o interfaz portable de sistema operativo para Unix) y no-POSIX, como Windows.

URL: http://isc.org/products/DHCP/

48.2. Equipamiento lógico necesario.

48.2.1. CentOS, Fedora™ y Red Hat™ Enterprise Linux.

Ejecute lo siguiente para instalar o actualizar todo necesario:

```
yum -y install dhcp
```

48.3. Modificaciones necesarias en el muro cortafuegos.

Por lo general, jamás se abren puertos de DHCP a las redes públicas. Es necesario abrir los puerto 67 y 68 (**BOOTPS** y **BOOTPC**) por UDP, tanto para trafico entrante como saliente.

48.3.1. Servicio iptables.

Asumiendo que el servicio funcionará a través de la interfaz **eth1**, puede utilizar el mandato **iptables** del siguiente modo:

```
iptables -A INPUT -i eth1 -p udp -m state --state NEW -m udp \
    --sport 67:68 --dport 67:68 -j ACCEPT
service iptables save
```

O bien edite el archivo **/etc/sysconfig/iptables**:

```
vim /etc/sysconfig/iptables
```

Y añada el siguiente contenido:

```
-A INPUT -i eth1 -p udp -m state --state NEW -m udp --sport 67:68 --dport 67:68 -j ACCEPT
```

Reinicie el servicio **iptables** a fin de que surtan efecto los cambios.

```
service iptables restart
```

48.3.2. Shorewall.

Edite el archivo **/etc/shorewall/interfaces**:

```
vim /etc/shorewall/interfaces
```

Asumiendo que el servicio funcionará a través de la interfaz eth1 (zona loc), añada la opción **dhcp** a las opciones de la interfaz sobre la cual funciona el servicio **dhcpd**. Esta opción, tras reiniciar el servicio **shorewall**, habilita las comunicaciones de entrada y salida, para DHCP.

```
###############################################################################
#ZONE   INTERFACE       BROADCAST       OPTIONS
net     eth0            detect          blacklist
loc     eth1            detect          dhcp,blacklist
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Reinicie el servicio **shorewall** a fin de que surtan efecto los cambios.

```
service shorewall restart
```

48.4. SELinux y el servicio dhcpd.

Se recomienda encarecidamente dejar activo SELinux y dejar como están las políticas predeterminadas.

Nota.

Lo siguiente sólo aplica para **CentOS 5** y **Red Hat Enterprise Linux 5**.

Si se desea **eliminar la protección** que brinda SELinux al servicio **dhcpd**, utilice el siguiente mandato.

```
setsebool -P dhcpd_disable_trans 1
```

Si se desea **eliminar la protección** que brinda SELinux al sistema para funcionar como **cliente DHCP**, utilice el siguiente mandato.

```
setsebool -P dhcpc_disable_trans 1
```

Ninguna de estás políticas existe en **CentOS 6** y **Red Hat Enterprise Linux 6**.

48.5. Iniciar, detener y reiniciar, el servicio dhcpd.

Para hacer que el servicio de **dhcpd** esté activo con el siguiente inicio del sistema, en todos los niveles de ejecución (2, 3, 4 y 5), ejecute lo siguiente:

```
chkconfig dhcpd on
```

Para iniciar por primera vez el servicio **dhcpd**, ejecute:

```
service dhcpd start
```

Para hacer que los cambios hechos a la configuración del servicio **dhcpd** surtan efecto, ejecute:

```
service dhcpd restart
```

Para detener el servicio **dhcpd**, ejecute:

```
service dhcpd stop
```

48.6. Procedimientos.

48.6.1. Archivo de configuración /etc/sysconfig/dhcpd.

En el caso de disponer múltiples dispositivos de red en el servidor, se recomienda que el servicio **dhcpd** solamente funcione a través de la interfaz de red utilizada por la LAN. Edite el archivo **/etc/sysconfig/dhcpd** y agregue el valor **eth0**, **eth1**, **eth2**, etc., como argumento(s) del parámetro **DHCPDARGS** o bien lo que corresponda a la interfaz desde la cual accede la red local.

Edite el archivo **/etc/sysconfig/dhcpd**:

```
vim /etc/sysconfig/dhcpd
```

Para el siguiente ejemplo, considerando que **eth1** es la interfaz correspondiente a la LAN:

```
# Command line options here
DHCPDARGS=eth1
```

48.6.2. Archivo de configuración dhcpd.conf.

Considerando **como ejemplo** que se tiene una red local con las siguientes características:

- Dirección IP del segmento de red: **172.16.1.0**
- Dirección IP de difusión: **172.16.1.15**
- Máscara de sub-red: **255.255.255.240** (28 bit)
- Puerta de enlace: **172.16.1.1**
- Servidor de nombres: **172.16.1.1**
- Servidor Wins: **172.16.1.1**
- Servidores de tiempo (**NTP**): recomendamos utilizar los de NTP.org —es decir 0.pool.ntp.org, 1.pool.ntp.org, 2.pool.ntp.org y 3.pool.ntp.org— los cuales son confiables y de acceso gratuito.
- Rango de direcciones IP a asignar de modo dinámico: **172.16.1.2 hasta 172.16.1.14.**

Nota.

Es indispensable **conocer y entender perfectamente**, todo lo anterior para poder continuar con este documento. Si se tienen dudas, por favor, primero consultar y estudiar, el documento titulado «**Introducción a IP versión 4**.»

Puede utilizar el contenido de ejemplo, que se encuentra más adelante, **para adaptar o bien crear desde cero,** un nuevo archivo de configuración para el servicio **dhcpd**, ajustando los datos a una red para un conjunto de sistemas en particular.

48.6.3. Configuración básica.

Descargue el archivo plantilla, con una configuración mínima recomendada, desde AlcanceLibre.org, ejecutando lo siguiente:

```
cd /etc/dhcp/
mv dhcpd.conf dhcpd.conf.original
wget http://www.alcancelibre.org/linux/secrets/dhcpd.conf
restorecon dhcpd.conf
cd
```

Si se utiliza **CentOS 6** o **Red Hat Enterprise Linux 6**, edite el archivo **/etc/dhcp/dhcpd.conf**.

```
vim /etc/dhcp/dhcpd.conf
```

Nota.

Si se utiliza **CentOS 5** o **Red Hat Enterprise Linux 5**, edite el archivo **/etc/dhcpd.conf**.

```
vim /etc/dhcpd.conf
```

Para efectos prácticos, utilice la siguiente plantilla y modifique todo lo que esté **resaltado**.

```
# Si se tienen problemas con equipos con Windows Vista/7/8 omita el parámetro
# server-identifier. Ésto aunque rompe con el protocolo DHCP, permite a los
# clientes Windows Vista/7/8 poder comunicarse con el servidor DHCP y aceptar
# la dirección IP proporcionada.
# server-identifier 172.16.1.1;
ddns-update-style interim;
ignore client-updates;
authoritative;
default-lease-time 900;
max-lease-time 7200;
option ip-forwarding off;
option domain-name "red-local.net";
option ntp-servers 0.pool.ntp.org, 1.pool.ntp.org, 2.pool.ntp.org, 3.pool.ntp.org;

shared-network redlocal {
         subnet 172.16.1.0 netmask 255.255.255.240 {
                  option routers 172.16.1.1;
                  option subnet-mask 255.255.255.240;
                  option broadcast-address 172.16.1.15;
                  option domain-name-servers 172.16.1.1;
                  option netbios-name-servers 172.16.1.1;
                  range 172.16.1.2 172.16.1.14;
         }
}
```

Lo anterior corresponde a la configuración básica recomendada para un servidor DHCP básico.

Una vez terminada la configuración, para iniciar el servicio ejecute:

```
service dhcpd start
```

48.6.4. Asignación de direcciones IP estáticas.

Para definir equipos con direcciones IP estáticas, pueden añadirse también en la configuración de la siguiente forma, especificando el nombre de anfitrión, dirección MAC y dirección IP:

```
        host impresora {
                option host-name "epl5900.red-local.net";
                hardware ethernet 00:24:2B:65:54:84;
                fixed-address 172.16.1.59;
                }
```

Edite el archivo **/etc/dhcp/dhcpd.conf** o bien **/etc/dhcpd.conf**, según corresponda:

```
vim /etc/dhcp/dhcpd.conf
```

Un ejemplo de la configuración quedaría del siguiente modo:

```
# Si se tienen problemas con equipos con Windows Vista/7/8 omita el parámetro
# server-identifier. Ésto aunque rompe con el protocolo DHCP, permite a los
# clientes Windows Vista/7/8 poder comunicarse con el servidor DHCP y aceptar
# la dirección IP proporcionada.
# server-identifier 172.16.1.1;
ddns-update-style interim;
ignore client-updates;
authoritative;
default-lease-time 900;
max-lease-time 7200;
option ip-forwarding off;
option domain-name "red-local.net";
option ntp-servers 0.pool.ntp.org, 1.pool.ntp.org, 2.pool.ntp.org, 3.pool.ntp.org;

shared-network redlocal {
         subnet 172.16.1.0 netmask 255.255.255.240 {
                  option routers 172.16.1.1;
                  option subnet-mask 255.255.255.240;
                  option broadcast-address 172.16.1.15;
                  option domain-name-servers 172.16.1.1;
                  option netbios-name-servers 172.16.1.1;
                  range 172.16.1.2 172.16.1.12;
         }
# Equipos con IP fija.
         host impresora {
                  option host-name "epl5900.red-local.net";
                  hardware ethernet 00:24:2B:65:54:84;
                  fixed-address 172.16.1.13;
                  }
         host pc14 {
                  option host-name "pc14.red-local.net";
                  hardware ethernet 00:50:BF:27:1C:1C;
                  fixed-address 172.16.1.14;
                  }
}
```

Si realizó cambios en la configuración, reinicie el servicio **dhcpd** a fin de que surtan efecto los cambios.

```
service dhcpd restart
```

48.6.5. Limitar el acceso por dirección MAC.

Es posible limitar el acceso al servidor DHCP a través de la opción **deny** con el valor **unknown-clients** y definiendo una lista de direcciones MAC. De tal modo, a los anfitriones que estén ausentes en dicha lista les será denegado el servicio. Ejemplo:

```
                deny unknown-clients;
                host impresora {
                        hardware ethernet 00:24:2B:65:54:84;
                }
                host pc1 {
                        hardware ethernet 00:50:BF:27:1C:1C;
                }
```

Edite el archivo **/etc/dhcp/dhcpd.conf** o bien **/etc/dhcpd.conf**, según corresponda:

```
vim /etc/dhcp/dhcpd.conf
```

Un ejemplo de la configuración quedaría del siguiente modo, donde sólo las direcciones MAC en la lista pueden conectarse hacia el servidor DHCP y recibir una dirección IP:

```
# Si se tienen problemas con equipos con Windows Vista/7/8 omita el parámetro
# server-identifier. Ésto aunque rompe con el protocolo DHCP, permite a los
# clientes Windows Vista/7/8 poder comunicarse con el servidor DHCP y aceptar
# la dirección IP proporcionada.
# server-identifier 172.16.1.1;
ddns-update-style interim;
ignore client-updates;
authoritative;
default-lease-time 900;
max-lease-time 7200;
option ip-forwarding off;
option domain-name "red-local.net";
option ntp-servers 0.pool.ntp.org, 1.pool.ntp.org, 2.pool.ntp.org, 3.pool.ntp.org;

shared-network redlocal {
         subnet 172.16.1.0 netmask 255.255.255.240 {
                  option routers 172.16.1.1;
                  option subnet-mask 255.255.255.240;
                  option broadcast-address 172.16.1.15;
                  option domain-name-servers 172.16.1.1;
                  option netbios-name-servers 172.16.1.1;
                  range 172.16.1.2 172.16.1.14;
         }
# Lista de direcciones MAC que tendrán permitido utilizar el servidor
# DHCP.
# deny unknown-clients impide que equipos fuera de esta lista puedan
# utilizar el servicio.
                  deny unknown-clients;
                  host impresora {
                           hardware ethernet 00:24:2B:65:54:84;
                  }
                  host pc1 {
                           hardware ethernet 00:50:BF:27:1C:1C;
                  }
                  host pc2 {
                           hardware ethernet F4:C7:14:70:FA:AC;
                  }
                  host laptop1 {
                           hardware ethernet 44:87:FC:AA:DD:2D;
                  }
                  host laptop2 {
                           hardware ethernet 70:F1:A1:9F:70:3B;
                  }
}
```

Si realizó cambios en la configuración, reinicie el servicio **dhcpd** a fin de que surtan efecto los cambios.

```
service dhcpd restart
```

48.6.6. Configuración para funcionar con DNS dinámico.

El servidor DNS puede funcionar de modo dinámico permitiendo la actualización en tiempo real de los nombres de anfitrión y las direcciones IP asociadas a éstos, a través de la información enviada a través de un servidor DHCP.

Edite el archivo **/etc/dhcp/dhcpd.conf**:

```
vim /etc/dhcp/dhcpd.conf
```

Asumiendo que ya se dispone de un servidor DNS previamente configurado y funcionando, para configurar el servidor DHCP a fin de que actualice automáticamente los registros correspondientes en las zonas del servidor DNS, sólo basta añadir los parámetros **ddns-updates**, **ddns-domainname**, **ddns-rev-domainname**, una inclusión para utilizar la misma firma digital de la configuración del DNS y definir las zonas de localhost, zona de re-envío y zona de resolución inversa del DNS, con los valores ejemplificados a continuación, solamente siendo necesario reemplazar **los valores resaltados**.

```
# Si se tienen problemas con equipos con Windows Vista/7/8 omita el parámetro
# server-identifier. Ésto aunque rompe con el protocolo DHCP, permite a los
# clientes Windows Vista/7/8 poder comunicarse con el servidor DHCP y aceptar
# la dirección IP proporcionada.
# server-identifier 172.16.1.1;
ddns-update-style interim;
ddns-updates on;
ddns-domainname "red-local.net.";
ddns-rev-domainname "in-addr.arpa.";
ignore client-updates;
authoritative;
default-lease-time 900;
max-lease-time 7200;
option ip-forwarding off;
option domain-name "red-local.net";
option ntp-servers 0.pool.ntp.org, 1.pool.ntp.org, 2.pool.ntp.org, 3.pool.ntp.org;

include "/etc/rndc.key";

zone localdomain. {
         primary 127.0.0.1;
         key rndc-key;
}
zone  1.16.172.in-addr.arpa. {
         primary 127.0.0.1;
         key rndc-key;
}
zone red-local.net. {
         primary 127.0.0.1;
         key rndc-key;
}

shared-network redlocal {
         subnet 172.16.1.0 netmask 255.255.255.240 {
                  option routers 172.16.1.1;
                  option subnet-mask 255.255.255.240;
                  option broadcast-address 172.16.1.15;
                  option domain-name-servers 172.16.1.1;
                  option netbios-name-servers 172.16.1.1;
                  range 172.16.1.2 172.16.1.14;
         }
}
```

Para que lo anterior funcione con el servidor DNS, considerando que ya están instalados los paquetes **bind** y **bind-chroot**, se requiere generar los archivos **red-local.net.zone** y **1.16.172.in-addr.arpa.zone**, dentro del directorio **/dynamic/**. Cambie al directorio **/dynamic/**:

```
cd /var/named/dynamic/
```

Utilice el mandato **touch** para crear los archivos **red-local.net.zone** y **1.16.172.in-addr.arpa.zone**:

```
touch red-local.net.zone
touch 1.16.172.in-addr.arpa.zone
```

Ambos archivos deben tener permisos de lectura y escritura para usuario y sólo lectura para grupo:

```
chmod 640 red-local.net.zone
chmod 640 1.16.172.in-addr.arpa.zone
```

Ambos archivos deben pertenecer al usuario **named** y grupo **named**.

```
chown named:named red-local.net.zone
chown named:named 1.16.172.in-addr.arpa.zone
```

Edite el archivo /var/named/dynamic/**red-local.net.zone**:

```
vim red-local.net.zone
```

Éste deberá tener el siguiente contenido, donde solamente será necesario añadir al ejemplo los registros de los equipos con IP fija:

```
$TTL 86400
@       IN      SOA     servidor.red-local.net. root.localhost. (
                        2011101901;
                        28800;
                        7200;
                        604800;
                        86400;
                        )
@               IN      NS      servidor.red-local.net.
servidor        IN      A       172.16.1.1
```

Edite el archivo /var/named/dynamic/**1.16.172.in-addr.arpa.zone**:

```
vim 1.16.172.in-addr.arpa.zone
```

Éste deberá tener el siguiente contenido, donde solamente será necesario añadir al ejemplo los registros de los equipos con IP fija:

```
$TTL 86400
@       IN      SOA     servidor.red-local.net. root.localhost. (
                        2011101901;
                        28800;
                        7200;
                        604800;
                        86400;
                        )
@               IN      NS      servidor.red-local.net.
1               IN      PTR     servidor.red-local.net.
```

Cambie al directorio **/etc/**:

```
cd /etc/
```

Edite el archivo **/etc/named.conf**:

```
vim named.conf
```

Éste deberá tener un contenido similar al siguiente:

```
options {
        directory "/var/named";
        dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        forwarders {
                8.8.8.8;
                8.8.4.4;
        };
        forward first;
// Sólo habilitar lo siguiente si se va a utilizar DNSSEC
// y si forwarders tienen soporte para DNSSEC.
        dnssec-enable no;
        dnssec-validation no;
//      dnssec-lookaside auto;
//      bindkeys-file "/etc/named.iscdlv.key";
};

include "/etc/rndc.key";

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
        category lame-servers { null; };
};

controls {
        inet 127.0.0.1 allow { 127.0.0.1; } keys { "rndc-key"; };
};

view "local" {
        match-clients { 127.0.0.0/8; 172.16.1.0/26; };
        recursion yes;
        include "/etc/named.rfc1912.zones";
        zone "." IN {
                type hint;
                file "named.ca";
        };
        zone "red-local.net" {
                type master;
                file "dynamic/red-local.net.zone";
                allow-update { key "rndc-key"; };
        };
        zone "1.16.172.in-addr.arpa" {
                type master;
                file "dynamic/1.16.172.in-addr.arpa.zone";
                allow-update { key "rndc-key"; };
        };
};

view "public" {
        match-clients { any; };
        recursion no;
        zone "." IN {
                type hint;
                file "named.ca";
        };
};
```

Regrese al directorio de inicio.

```
cd
```

Active la política de SELinux, la cual permitirá al servidor DNS poder realizar modificaciones a los archivos de zona.

```
setsebool -P named_write_master_zones 1
```

Reinicie el servicio **named** a fin de que surtan efecto los cambios.

```
service named restart
```

Reinicie también el servicio **dhcpd** a fin de que surtan efecto los cambios y para que el servidor DHCP comience a interactuar con el servidor DNS.

```
service dhcpd restart
```

A partir de este momento, todo cliente que tenga definido en su configuración local un nombre de anfitrión y al cual le sea asignada una dirección IP a través del servidor DHCP recién configurado, comunicará su nombre de anfitrión al servidor DHCP, el cual a su vez comunicará al servidor DNS este mismo nombre asociada a la dirección IP asignada al cliente, de modo que el DNS añadirá automáticamente el registro correspondiente a las zonas de re-envío y de resolución inversa correspondientes.

Verifique que el servidor DNS dinámico funciona correctamente, simulando lo que en adelante hará automáticamente en segundo plano el servidor DHCP, añadiendo un par de registros a través del mandato **nsupdate**. Ejecute lo siguiente para conectarse al servidor DNS utilizando la firma digital que utilizarán tanto el éste como el servidor DHCP:

```
nsupdate -k /etc/rndc.key
```

Desde el intérprete de mandatos de **nsupdate**, ejecute lo siguiente:

```
server 127.0.0.1
update add prueba.red-local.net. 86400 A 172.16.1.14
send
update add 14.1.16.172.in-addr.arpa. 86400 PTR prueba.red-local.net.
send
quit
```

Si lo anterior devuelve errores como el siguiente:

```
update failed: REFUSED
```

Significa que hay errores en el procedimiento realizado o la configuración o bien que la firma digital utilizada en el archivo **/etc/named.conf** es distinta a la del archivo **/etc/rndc.key**.

Si lo anterior devuelve errores como el siguiente:

```
; TSIG error with server: tsig indicates error
update failed: REFUSED(BADKEY)
```

Significa que el nombre de anfitrión pertenece a un dominio distinto al configurado o bien la dirección IP pertenece a otro bloque direcciones distinto al configurado. Corrija lo necesario si así es el caso.

Si el procedimiento concluyó sin errores, haga consultas al servidor DNS para **prueba.red-local.net** y **172.16.1.14** para cotejar que el servidor DNS aceptó los dos registros añadidos a través de **nsupdate**, ejecutando lo siguiente:

```
host prueba.red-local.net
host 172.16.1.14
```

Lo anterior debe devolver una salida similar a la siguiente:

```
[root@servidor ~]# host prueba.red-local.net
prueba.red-local.net has address 172.16.1.14
[root@servidor ~]# host 172.16.1.14
14.1.16.172.in-addr.arpa domain name pointer prueba.red-local.net.
```

Si la salida devuelve errores, significa que hay errores en el procedimiento realizado o bien el dominio y zona de resolución inversa son diferentes a los configurados. Corrija lo necesario si así es el caso.

Si el procedimiento concluyó correctamente, utilice el mandato **nsupdate** para conectarse de nuevo al servidor DNS ejecutando lo siguiente:

```
nsupdate -k /etc/rndc.key
```

Desde el intérprete de mandatos de **nsupdate**, ejecute lo siguiente para eliminar los registros:

```
server 127.0.0.1
update delete prueba.red-local.net. A
send
update delete 14.1.16.172.in-addr.arpa. PTR
send
quit
```

Esta es, por cierto, la metodología recomendada para añadir o eliminar registros de zonas en el servidor DNS cuando se utilizan zonas dinámicas.

48.7. Comprobaciones desde cliente DHCP.

Hecho lo anterior, solamente se necesitará configurar como interfaces DHCP, las utilizadas en las estaciones de trabajo que sean necesarias, sin importar que sistema operativo utilicen.

Después concluida la configuración y que estén funcionando los servicio correspondientes, pueden hacerse comprobaciones desde un cliente GNU/Linux, es decir, **desde otro equipo**. Abra una terminal, como usuario root y, asumiendo que se tiene una interfaz de red denominada **eth0**, utilice los siguientes mandatos para desactivar la interfaz **eth0** y asignar una nueva dirección **IP** a través del servidor **dhcp**.

```
ifdown eth0
dhclient -d -I nombre-equipo -H nombre-equipo eth0
```

Lo anterior deberá devolver el mensaje «Determinando la información IP para eth0...» y el símbolo de sistema. Para corroborar, utilice el mandato **ifconfig** para visualizar los dispositivos de red activos en el sistema. Pulse **CTRL-C** para terminar el programa.

Si se dispone de varios servidores DHCP y se desea probar la configuración de alguno en particular, puede añadir la opción **-V** al mandato **dhclient**, definiendo como valor para esta opción, el mismo valor que fue asignado para el parámetro **server-identifier**, establecido en el archivo **/etc/dhcp/dhcpd.conf** del servidor correspondiente.

```
ifdown eth0
dhclient -d -I nombre-equipo -H nombre-equipo -V 172.16.1.1 eth0
```

Edite el archivo **/etc/sysconfig/network-scripts/ifcfg-eth0** o el que corresponda al dispositivo de red principal del sistema cliente:

```
vim /etc/sysconfig/network-scripts/ifcfg-eth0
```

La configuración permanente del dispositivo de red, considerando **como ejemplo** la interfaz eth0 con dirección **MAC** 00:01:03:DC:67:23, solicitando los datos para los servidores **DNS**, puerta de enlace y servidores de tiempo, sería la siguiente:

```
DEVICE=eth0
ONBOOT=yes
USERCTL=yes
HWADDR=00:01:03:DC:67:23
TYPE=Ethernet
NM_CONTROLLED=no
BOOTPROTO=dhcp
DEFROUTE=yes
PEERDNS=yes
PEERROUTES=yes
PEERNTP=yes
DOMAIN=red-local.net
DHCP_CLIENT_ID=nombre-equipo
DHCP_HOSTNAME=nombre-equipo
```

Si utiliza **NM_CONTROLLED=yes**, deje que el servicio **NetworkManager** se encargue por si solo de aplicar los cambios. Si utiliza **NM_CONTROLLED=no**, reinicie el servicio **network** a fin de que surtan efecto los cambios.

```
service network restart
```

49. Instalación y configuración de vsftpd.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

49.1. Introducción.

49.1.1. Acerca del protocolo FTP.

FTP (***F****ile* ***T****ransfer* ***P****rotocol*) o Protocolo de Transferencia de Archivos (o archivos informáticos) es uno de los protocolos estándar más utilizados en Internet siendo el más idóneo para la transferencia de grandes bloques de datos a través de redes que soporten TCP/IP. El servicio utiliza los puertos 20 y 21, exclusivamente sobre TCP. El puerto 20 es utilizado para el flujo de datos entre cliente y servidor. El puerto 21 es utilizando para el envío de órdenes del cliente hacia el servidor. Prácticamente todos los sistemas operativos y plataformas incluyen soporte para FTP, lo que permite que cualquier computadora conectada a una red basada sobre TCP/IP pueda hacer uso de este servicio a través de un cliente FTP.

Existen dos métodos, el modo activo y el modo pasivo.

URL: http://tools.ietf.org/html/rfc959

49.1.1.1. Modo activo.

En este modo, el cliente crea una conexión de datos a través del puerto 20 del servidor, mientras que en el cliente asocia esta conexión desde un puerto aleatorio entre 1024 y 65535, enviando el mandato PORT para indicar al servidor el puerto a utilizar para la transferencia de datos. Tiene como desventaja que el cliente FTP debe estar dispuesto a aceptar cualquier conexión de entrada asociada a puertos entre 1024 y 65535, lo que significa que el cliente tendría que estar detrás de un muro cortafuegos que acepte establecer conexiones entrantes en este rango de puertos o bien acceder hacia Internet sin un muro cortafuegos de por medio, lo que evidentemente implica un enorme riesgo de seguridad. El modo activo sólo es conveniente en la ausencia de un muro cortafuegos entre el servidor y el cliente, como ocurre en los escenarios de una red de área local.

49.1.1.2. Modo pasivo.

Fue creado como una alternativa al problema que representa el modo activo. A diferencia de éste último, el modo pasivo envía un mandato PASV en lugar del mandato PORT a través del puerto de control del servidor. Éste devuelve como respuesta el número de puerto a través del cual debe conectarse el cliente para hacer la transferencia de datos. El servidor puede elegir al azar cualquier puerto entre 1024 y 65535 o bien el rango de puertos determinado por el administrador del sistema. En el caso de **Vsftpd**, se puede definir un rango arbitrario de puertos para conexiones pasivas utilizando las opciones **pasv_min_port** y **pasv_max_port**. Éste es el método recomendado para servidores de acceso público.

49.1.2. Acerca del protocolo FTPS.

FTPS (también referido como **FTP/SSL**) es la forma de designar diferentes formas a través de las cuales se pueden realizar transferencias seguras de archivos a través de **FTP** utilizando **SSL** o **TLS**. Son mecanismos muy diferentes a los del protocolo SFTP (***S**SH **F**ile **T**ransfer **P**rotocol*).

Existen dos diferentes métodos para realizar una conexión **SSL/TLS** a través de **FTP**. La primera y más antigua es a través del **FTPS Implícito** (*Implicit FTPS*), que consiste en cifrar la sesión completa a través de los puertos 990 (FTPS) y 998 (FTPS Data), sin permitir negociación con el cliente, el cual está obligado a conectarse directamente al servidor FTPS con el inicio de sesión **SSL/TLS**. El segundo método, que es el recomendado por el RFC 4217 y el utilizado por **Vsftpd**, es **FTPS Explícito** (*Explicit FTPS* o **FTPES**), donde el cliente realiza la conexión normal a través del puerto 21 y permitiendo negociar, de manera opcional, una conexión **TLS**.

49.1.3. Acerca de RSA.

RSA, acrónimo de los apellidos de sus autores, Ron **R**ivest, Adi **S**hamir y Len **A**dleman, es un algoritmo para cifrar claves públicas, el cual fue publicado en 1977 y patentado 1983, en EE.UU., por el Instituto Tecnológico de Michigan (**MIT**). **RSA** es utilizado en todo el mundo para los protocolos destinados para el comercio electrónico.

URL: http://es.wikipedia.org/wiki/RSA

49.1.4. Acerca de OpenSSL.

OpenSSL es una implementación libre, de código fuente abierto, de los protocolos **SSL** (**S**ecure **S**ockets **L**ayer o Nivel de Zócalo Seguro) y **TLS** (***T**ransport **L**ayer **S**ecurity o Seguridad para Nivel de Transporte). Está basado sobre el extinto proyecto **SSLeay**, iniciado por Eric Young y Tim Hudson, hasta que éstos comenzaron a trabajar para la división de seguridad de EMC Corporation.*

URL: http://www.openssl.org/

49.1.5. Acerca de X.509.

X.509 es un estándar **ITU-T** (estandarización de **T**elecomunicaciones de la ***I**nternational **T**elecommunication **U**nion*) para infraestructura de claves públicas (**PKI** o ***P**ublic **K**ey **I**nfrastructure*). Entre otras cosas, establece los estándares para certificados de claves públicas y un algoritmo, para validación de ruta de certificación. Este último se encarga de verificar que la ruta de un certificado sea válida bajo una infraestructura de clave pública determinada. Es decir, desde el certificado inicial, pasando por certificados intermedios, hasta el certificado de confianza emitido por una Autoridad Certificadora (**CA** o **C**ertification **A**uthority).

URL: http://es.wikipedia.org/wiki/X.509

49.1.6. Acerca de vsftpd.

Vsftpd (***V**ery **S**ecure **FTP** **D**aemon*) es un equipamiento lógico utilizado para implementar servidores de archivos a través del protocolo **FTP**. Se distingue principalmente porque sus valores predeterminados son muy seguros y por su sencillez en la configuración, comparado con otras alternativas como ProFTPD y Wu-ftpd. Actualmente se presume que vsftpd podría ser quizá el servidor **FTP** más seguro del mundo.

URL: http://vsftpd.beasts.org/

49.2. Equipamiento lógico necesario.

49.2.1. Instalación a través de yum.

Ejecute lo siguiente desde una terminal si utiliza **CentOS**, **Fedora™** o **Red Hat™ Enterprise Linux**:

```
yum -y install vsftpd
```

49.3. Archivos de configuración.

/etc/vsftpd/chroot_list

Lista que definirá usuarios a enjaular o no a enjaular, dependiendo de la configuración.

/etc/vsftpd/vsftpd.conf

Archivo de configuración de VSFTPD.

El archivo **/etc/vsftpd/chroot_list** es inexistente, por lo cual es conveniente crearlo antes de comenzar a trabajar con la configuración. Por favor ejecute lo siguiente antes de continuar:

```
touch /etc/vsftpd/chroot_list
```

49.3.1. Iniciar, detener y reiniciar el servicio vsftpd.

Ejecute lo siguiente para iniciar por primera vez el servicio **vsftpd**:

```
service vsftpd start
```

Ejecute lo siguiente para reiniciar el servicio **vsftpd** o bien hacer que los cambios hechos a la configuración surtan efecto:

```
service vsftpd restart
```

Ejecute lo siguiente para detener el servicio **vsftpd**:

```
service vsftpd stop
```

49.3.2. Agregar el servicio vsftpd al arranque del sistema.

Ejecute lo siguiente para hacer que el servicio de **vsftpd** esté activo con el siguiente inicio del sistema, en todos los niveles de ejecución (2, 3, 4 y 5):

```
chkconfig vsftpd on
```

49.4. Modificaciones necesarias en el muro cortafuegos.

Es necesario abrir los puerto 20 y 21, por TCP (**FTP-DATA** y **FTP**, respectivamente) y el rango de puertos para conexiones pasivas que se haya definido.

49.4.1. Servicio iptables.

Ejecute lo siguiente para anexar las reglas de **iptables** correspondientes:

```
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 20 -j ACCEPT
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 30300:30309 -j ACCEPT
```

Ejecute lo siguiente para guardar los cambios:

```
service iptables save
```

O bien añada lo siguiente al archivo **/etc/sysconfig/iptables**:

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 20 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 30300:30309 -j ACCEPT
```

Y reinicie el servicio **iptables**:

```
service iptables restart
```

49.4.2. Shorewall.

Edite el archivo **/etc/shorewall/rules**:

```
vi /etc/shorewall/rules
```

Las reglas corresponderían a algo similar a lo siguiente, permitiendo el acceso hacia el servicio FTP desde cualquier zona del muro cortafuegos:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  all     fw      tcp     20,21,30300:30309
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Ejecute lo siguiente al terminar de configurar las reglas para **Shorewall** a fin de reiniciar el muro cortafuegos:

```
service shorewall restart
```

49.5. Procedimientos.

49.5.1. SELinux y el servicio vsftpd.

SELinux controla varias funciones de el servicio **vsftpd** incrementando el nivel de seguridad de éste.

Ejecute lo siguiente para permitir que el servidor FTP pueda asociarse a cualquier puerto sin reservar al funcionar en modo pasivo:

```
setsebool -P ftpd_use_passive_mode 1
```

Ejecute lo siguiente para permitir que los usuarios anónimos puedan realizar procesos de escritura sobre el sistema de archivos:

```
setsebool -P allow_ftpd_anon_write 1
```

Si se necesita permitir el acceso utilizando las cuentas de usuarios del anfitrión local, a fin de que éstos puedan acceder a sus directorio de inicio, se debe habilitar la política **ftp_home_dir**:

```
setsebool -P ftp_home_dir 1
```

Ejecute lo siguiente para hacer que SELinux permita acceder a los usuarios locales al resto del sistema de archivos:

```
setsebool -P allow_ftpd_full_access 1
```

Ejecute lo siguiente para permitir que el servicio **vsftpd** pueda hacer uso de sistemas de archivos remotos a través de CIFS (Samba) o NFS y que serán utilizados para compartir a través del servicio:

```
setsebool -P allow_ftpd_use_cifs 1
setsebool -P allow_ftpd_use_nfs 1
```

Nota.

Lo siguiente sólo aplica para **CentOS 5** y **Red Hat™ Enterprise Linux 5**.

Ejecute lo siguiente para eliminar por completo la protección que brinda SELinux al servicio **vsftpd** y que éste funcione normalmente sin esta valiosa protección, haciendo que todo lo anteriormente descrito en esta sección pierda sentido:

```
setsebool -P ftpd_disable_trans 1
```

Esta política es inexistente en **CentOS 6** y **Red Hat™ Enterprise Linux 6**.

49.5.2. Archivo /etc/vsftpd/vsftpd.conf.

Utilice un editor de texto y modifique el archivo **/etc/vsftpd/vsftpd.conf**.

```
vi /etc/vsftpd/vsftpd.conf
```

A continuación analizaremos las opciones a modificar o añadir según se requiera para necesidades particulares.

49.5.3. Opción anonymous_enable.

Esta opción viene incluida en la configuración predeterminada. Se utiliza para definir si se permitirán los accesos anónimos al servidor. Establezca como valor **YES** o **NO** de acuerdo a lo que se requiera.

```
anonymous_enable=YES
```

49.5.4. Opción local_enable.

Esta opción viene incluida en la configuración predeterminada. Establece si se van a permitir los accesos autenticados de los usuarios locales del sistema. Establezca como valor **YES** o **NO** de acuerdo a lo que se requiera.

```
local_enable=YES
```

49.5.5. Opción write_enable.

Esta opción viene incluida en la configuración predeterminada. Establece si se permite el mandato **write** (escritura) en el servidor. Establezca como valor **YES** o **NO** de acuerdo a lo que se requiera.

```
write_enable=YES
```

49.5.6. Opciones anon_upload_enable y anon_mkdir_write_enable

Ambas opciones vienen incluidas en la configuración predeterminada.

La opción **anon_upload_enable** específica si los usuarios anónimos tendrán permitido subir contenido al servidor. Por lo general no es una función deseada, por lo que se acostumbra desactivar ésta.

```
anon_upload_enable=NO
```

La opción **anon_mkdir_write_enable** específica si los usuarios anónimos tendrán permitido crear directorios en el servidor. Al igual que la anterior, por lo general no es una función deseada, por lo que se acostumbra desactivar ésta.

```
anon_mkdir_write_enable=NO
```

Nota.

Si se desea que los usuarios anónimos puedan subir archivos al servidor FTP, se deben dejar estas dos opciones con valor **YES**, guardar el archivo **/etc/vsftpd/vsftpd.conf** y regresar al intérprete de mandatos para crear un directorio denominado **/var/ftp/incoming**, el cual debe pertenecer al usuario y grupo **ftp** y tener contexto de SELinux tipo **public_content_rw_t**.

```
mkdir /var/ftp/incoming
chown ftp:ftp /var/ftp/incoming
chcon -R -t public_content_rw_t /var/ftp/incoming
```

Se recomienda que **/var/ftp/incoming** esté asignado como una partición independiente al resto del sistema o bien se le aplique cuota de disco al usuario **ftp**, porque de otro modo cualquiera podría fácilmente saturar el espacio de disco disponible, desencadenando una denegación de servicio en el servidor.

49.5.7. Opción ftpd_banner.

Esta opción viene incluida en la configuración predeterminada. Sirve para establecer el banderín de bienvenida que será mostrado cada vez que un usuario acceda al servidor. Puede establecerse cualquier frase breve que considere conveniente, pero **sin signos de puntuación**.

```
ftpd_banner=Bienvenido al servidor FTP de nuestra empresa
```

49.5.8. Estableciendo jaulas para los usuarios: opciones chroot_local_user y chroot_list_file.

Estas opciones vienen incluidas en la configuración predeterminada.

De modo predeterminado los usuarios del sistema que se autentiquen tendrán acceso a otros directorios del sistema fuera de su directorio personal. Si se desea limitar a los usuarios a sólo poder utilizar su propio directorio personal, puede hacerse fácilmente con la opción **chroot_local_user** que habilitará la función de **chroot()** y las opciones **chroot_list_enable** y **chroot_list_file**, para establecer el archivo con la lista de usuarios que quedarán excluidos de la función **chroot()**.

```
chroot_local_user=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/chroot_list
```

Con lo anterior, cada vez que un usuario local se autentique en el servidor FTP, sólo tendrá acceso a su propio directorio personal y lo que éste contenga. Por favor **recuerde crear el archivo /etc/vsftpd/chroot_list** debido a que de otro modo será imposible que funcione correctamente el servicio vsftpd.

Nota.

Cabe señalar que la función **chroot()** puede ser peligrosa si el usuario regular utilizado tiene acceso al intérprete de mandatos del sistema (**/bin/bash** o **/bin/sh**) y además privilegios de escritura sobre el directorio raíz de su propia jaula (es decir su directorio de inicio). Los directorios de inicio de los usuarios involucrados deben tener permiso 755, sean propiedad de root y se asigne al usuario **/bin/false** o **/sbin/nologin** como intérprete de mandatos.

Lo siguiente corresponde a lo que sería necesario ejecutar para modificar una cuenta de usuario regular para la cual se quiera acceder al servidor FTP utilizando **chroot()** con vsftpd-3.x:

```
chmod 755 /home/mengano
chown root:root /home/mengano
mkdir /home/mengano/uploads
chown mengano:mengano /home/mengano/uploads
usermod -s /sbin/nologin mengano
```

Vsftpd impide desde la versión 3.0 el ingreso con **chroot()** a todos los usuarios regulares que tengan acceso al intérprete de mandatos o bien que posean privilegios de escritura sobre su propio directorio de inicio.

49.5.9. Opciones pasv_min_port y pasv_max_port.

Ambas opciones están ausentes en el archivo **/etc/vsftpd/vsftpd.conf**. **Añada éstas al final del archivo de configuración**. Permiten establecer el rango arbitrario de puertos utilizados para las conexiones pasivas. Puede elegirse cualquier rango de puertos entre 1024 y 65535, mismo que deberá ser habilitado en el muro cortafuegos del servidor. En el siguiente ejemplo se establece el rango de puertos para conexiones pasivas de 30300 a 30309:

```
pasv_min_port=30300
pasv_max_port=30309
```

49.5.10. Control del ancho de banda.

49.5.10.1. Opción anon_max_rate.

Esta opción **está ausente** en la configuración predeterminada. Puede añadirla al final del archivo **/etc/vsftpd/vsftpd.conf**. Se utiliza para limitar la tasa de transferencia, en bytes por segundo, para los usuarios anónimos, algo sumamente útil en servidores FTP de acceso público. En el siguiente ejemplo se limita la tasa de transferencia a 500 Kb por segundo para los usuarios anónimos:

```
anon_max_rate=524288
```

49.5.10.2. Opción local_max_rate.

Esta opción **está ausente** en la configuración predeterminada. Puede añadirla al final del archivo **/etc/vsftpd/vsftpd.conf**. Hace lo mismo que **anon_max_rate**, pero aplica para usuarios locales del servidor. En el siguiente ejemplo se limita la tasa de transferencia a 1 MB por segundo para los usuarios locales:

```
local_max_rate=1048576
```

49.5.10.3. Opción max_clients.

Esta opción **está ausente** en la configuración predeterminada. Puede añadirla al final del archivo **/etc/vsftpd/vsftpd.conf**. Establece el número máximo de clientes que podrán acceder simultáneamente hacia el servidor FTP. En el siguiente ejemplo se limitará el acceso a 20 clientes simultáneos.

```
max_clients=20
```

49.5.10.4. Opción max_per_ip.

Esta opción **está ausente** en la configuración predeterminada. Puede añadirla al final del archivo **/etc/vsftpd/vsftpd.conf**. Establece el número máximo de conexiones que se pueden realizar desde una misma dirección IP. Tome en cuenta que algunas redes acceden a través de un servidor intermediario (Proxy) o puerta de enlace y debido a ésto podrían quedar bloqueados innecesariamente algunos accesos. En el siguiente ejemplo se limita el número de conexiones por IP simultáneas a un máximo de 10.

```
max_per_ip=10
```

49.5.10.5. Soporte SSL/TLS.

Siendo que todos los datos enviados a través del protocolo FTP se hacen en texto simple (incluyendo nombres de usuario y claves de acceso), hoy en día es muy peligroso operar un servidor FTP sin SSL/TLS.

VSFTPD puede ser configurado fácilmente para utilizar los protocolos **SSL** (**S**ecure **S**ockets **L**ayer o Nivel de Zócalo Seguro) y **TLS** (**T**ransport **L**ayer **S**ecurity o Seguridad para Nivel de Transporte) a través de un certificado **RSA**.

Acceda al sistema como el usuario **root**.

Acceda al directorio **/etc/pki/tls/**.

```
cd /etc/pki/tls/
```

El certificado y firma digital se pueden generar utilizando el siguiente mandato, para lo cual se utilizará una estructura **X.509**, algoritmo de cifrado **RSA** de 2048 bits, sin **Triple DES**, el cual permita iniciar normalmente, sin interacción alguna, al servicio **vsftpd**, con una validez por **1825** días (cinco años). Ejecute lo siguiente:

```
openssl req -x509 -nodes -days 1825 -newkey rsa:2048 \
    -keyout private/vsftpd.key \
    -out certs/vsftpd.crt
```

Lo anterior solicitará se ingresen los siguientes datos:

- Código de dos letras para el país.
- Estado o provincia.
- Ciudad.
- Nombre de la empresa o bien la razón social.
- Unidad o sección responsable del certificado.
- Nombre del anfitrión (FQDN) o bien dominio con comodín.
- Dirección de correo electrónico de la persona responsable del certificado.

La salida devuelta sería similar a la siguiente:

```
You are about to be asked to enter information that will be
incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or
a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

-----
Country Name (2 letter code) [GB]:MX
State or Province Name (full name) [Berkshire]:Distrito Federal
Locality Name (eg, city) [Newbury]:Mexico
Organization Name (eg, company) [My Company Ltd]:Empresa, S.A. de C.V.
Organizational Unit Name (eg, section) []:Direccion Comercial
Common Name (eg your name or your server's hostname) []:*.dominio.org
Email Address []:webmaster@dominio.org
```

El archivo del certificado (**vsftpd.crt**) y el de la firma digital (**vsftpd.key**), deben tener permisos de sólo lectura para el usuario root.

```
chmod 400 certs/vsftpd.crt private/vsftpd.key
```

Regrese al directorio de inicio del usuario **root**.

```
cd
```

Edite el archivo **/etc/vsftpd/vsftpd.conf**:

```
vi /etc/vsftpd/vsftpd.conf
```

Añada al final de este archivo todo el siguiente contenido:

```
# Habilita el soporte de TLS/SSL
ssl_enable=YES
# Deshabilita o habilita utilizar TLS/SSL con usuarios anónimos
allow_anon_ssl=NO
# Obliga a utilizar TLS/SSL para todas las operaciones, es decir,
# transferencia de datos y autenticación de usuarios locales.
# Establecer el valor NO, hace que sea opcional utilizar TLS/SSL.
force_local_data_ssl=YES
force_local_logins_ssl=YES
# Se prefiere TLSv1 sobre SSLv2 y SSLv3
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
# Rutas del certificado y firma digital
rsa_cert_file=/etc/pki/tls/certs/vsftpd.crt
rsa_private_key_file=/etc/pki/tls/private/vsftpd.key
# Los desarrolladores de FileZilla decidieron con la versión 3.5.3 que
# eliminarían el soporte para el algoritmo de cifrado 3DES-CBC-SHA,
# con el argumento de que este algoritmo es una de los más lentos.
# Sin embargo con ésto rompieron compatibilidad con miles de
# servidores FTP que utilizan FTPES. La solución temporal, mientras
# los desarrolladores de FileZilla razonan lo absurdo de su
# decisión, es utilizar la siguiente opción:
ssl_ciphers=HIGH
# Filezilla además requiere desactivar la siguiente opción que puede
# romper compatibilidad con otros clientes. Cabe señalar que Filezilla
# se ha convertido en un desarrollo políticamente incorrecto por dejar
# de respetar los estándares.
require_ssl_reuse=NO
```

Una vez concluida la configuración, reinicie el servicio **vsftpd** ejecutando el siguiente mandato:

```
service vsftpd restart
```

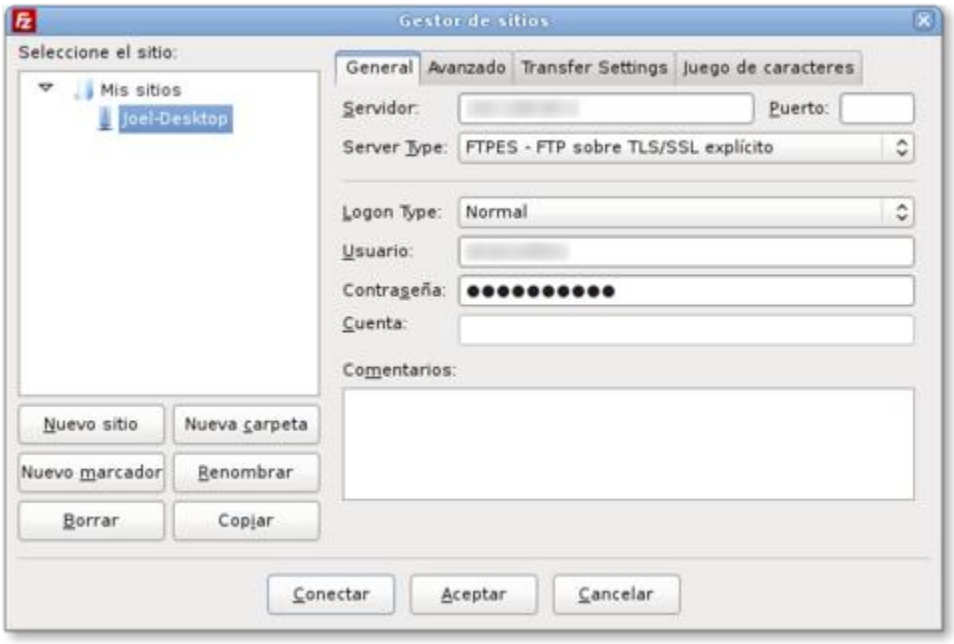
49.5.10.6. Clientes recomendados para acceder a FTPES.

Entre los clientes recomendados para acceder a través de **FTPES**, está **LFTP** (compilado con la opción *--with-openssl* y ejecutando con las opciones *-e 'set ftp:ssl-force true' -e 'set ssl:verify-certificate no'*). Ejemplo, asumiendo que se iniciará una conexión hacia el anfitrión 192.168.70.105:

```
lftp -e 'set ftp:ssl-force true' \
    -e 'set ssl:verify-certificate no' 192.168.70.105
```

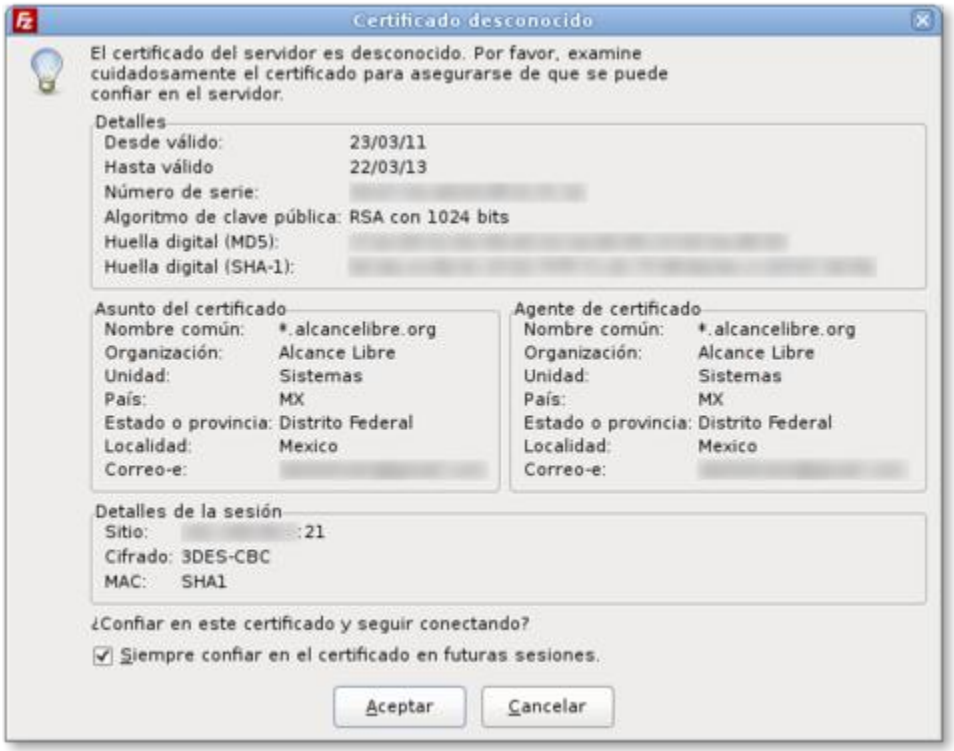
Filezilla 3.3.x (configurar conexión como *FTPES - FTP sobre TLS/SSL explícito*) y **WinSCP**. Al momento de redactar este documento, las versiones mas recientes de clientes como FireFTP o gFTP, tienen roto el soporte para FTP sobre TLS/SSL (**FTPS** y **FTPES**), por lo que por el momento es preferible evitarlos.

Si utiliza **Filezilla** es importante resaltar que a partir de la **versión 3.5.3** los desarrolladores tomaron una absurda decisión que eliminó el soporte para el algoritmo de cifrado SSL **3DES-CBC-SHA**, rompiendo la compatibilidad con miles de servidores FTP que utilizan **FTPES**. La solución a este problema es añadir la opción **ssl_ciphers=HIGH** en el archivo **/etc/vsftpd/vsftpd.conf**. **Filezilla** dispone de versiones para **GNU/Linux**, **Mac OS X** y **Windows XP/Vista/7**. La siguiente imagen ilustra la configuración que se requiere utilizar.



Configuración de cuenta FTPES en Filezilla.

Luego de iniciada la conexión, la primera vez que **Filezilla** se conecte al servidor, mostrará una ventana con la información del certificado y solicitará se acepte éste. Active la casilla que dice *«Siempre confiar en el certificado en futuras sesiones»* antes de hacer clic en el botón de *«Aceptar.»*



Dialogo de certificado de FTPES en Filezilla.

50. Configuración de OpenSSH.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

50.1. Introducción.

50.1.1. Acerca de SSH.

SSH (**S**ecure **Sh**ell) es un conjunto de estándares y protocolo de red que permite establecer una comunicación a través de un canal seguro entre un cliente local y un servidor remoto. Utiliza una clave pública cifrada para autenticar el servidor remoto y, de manera opcional, permitir al servidor remoto autenticar al usuario. SSH provee confidencialidad e integridad en la transferencia de los datos utilizando criptografía y **MAC** (**M**essage **A**uthentication **C**odes o Códigos de Autenticación de Mensaje). De modo predeterminado, escucha peticiones a través del puerto 22 por TCP.

50.1.2. Acerca de SFTP.

SFTP (**S**SH **F**ile **T**ransfer **P**rotocol) es un protocolo que provee funcionalidad de transferencia y manipulación de archivos a través de un flujo confiable de datos. Comúnmente se utiliza con **SSH** para proveer a éste de transferencia segura de archivos.

50.1.3. Acerca de SCP.

SCP (**S**ecure **C**o**p**y o Copia Segura) es una protocolo seguro para transferir archivos entre un anfitrión local y otro remoto, a través de **SSH**. Básicamente, es idéntico a **RCP** (**R**emote **C**o**p**y o Copia Remota), con la diferencia de que los datos son cifrados durante la transferencia para evitar la extracción potencial de información a través de programas de captura de las tramas de red (**packet sniffers**). **SCP** sólo implementa la transferencia de archivos, pues la autenticación requerida es realizada a través de **SSH**.

50.1.4. Acerca de OpenSSH.

OpenSSH (**Open S**ecure **Sh**ell) es una alternativa de código fuente abierto, con **licencia BSD**, hacia la implementación propietaria y de código cerrado **SSH** creada por **Tatu Ylönen**. **OpenSSH** es un proyecto creado por el equipo de desarrollo de OpenBSD y actualmente dirigido por **Theo de Raadt**. Se considera es más segura que la versión privativa Ylönen, gracias a la constante auditoría que se realiza sobre el código fuente por parte de una enorme comunidad de desarrolladores, una ventaja que brinda el *Software Libre*.

OpenSSH incluye servicio y clientes para los protocolos **SSH**, **SFTP** y **SCP**.

URL: http://www.openssh.org/.

50.2. Equipamiento lógico necesario.

50.2.1. En CentOS, Fedora™ y Red Hat™ Enterprise Linux.

Si realizó una instalación mínima, ejecute lo siguiente para instalar la paquetería necesaria:

```
yum -y install openssh openssh-server openssh-clients
```

50.2.2. En openSUSE™ y SUSE™ Linux Enterprise.

Si realizó una instalación mínima, ejecute lo siguiente para instalar la paquetería necesaria:

```
yast -i openssh
```

50.3. Activar, desactivar, iniciar, detener y reiniciar el servicio ssh.

De modo predeterminado, el servicio **sshd** está activo en los niveles de ejecución 2, 3, 4 y 5.

50.3.1. En CentOS, Fedora™ y Red Hat™ Enterprise Linux.

Para desactivar el servicio **sshd** de todos los niveles de ejecución ejecute:

```
chkconfig sshd off
```

Para iniciar por primera vez el servicio **sshd** ejecute:

```
service sshd start
```

Para hacer que surtan efecto los cambios hechos a la configuración del servicio **sshd** ejecute:

```
service sshd restart
```

Para detener el servicio **sshd** ejecute:

```
service sshd stop
```

50.3.2. En openSUSE™ y SUSE™ Linux Enterprise.

Para desactivar el servicio **sshd** de todos los niveles de ejecución ejecute:

```
insserv -r sshd
```

Para iniciar por primera vez el servicio **sshd** ejecute:

```
rcsshd start
```

Para hacer que surtan efecto los cambios hechos a la configuración del servicio **sshd** ejecute:

```
rcsshd restart
```

Para detener el servicio **sshd** ejecute:

```
service sshd stop
```

50.4. Modificaciones necesarias en el muro cortafuegos.

Es necesario abrir el puerto 22 por TCP (**SSH**) o bien el puerto que se haya seleccionado para el servicio.

50.4.1. En CentOS, Fedora™ y Red Hat™ Enterprise Linux.

50.4.1.1. Servicio iptables.

Puede utilizar el mandato **iptables** del siguiente modo:

```
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
service iptables save
```

O bien añada lo siguiente al archivo **/etc/sysconfig/iptables**:

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
```

Y reinicie el servicio **iptables**:

```
service iptables restart
```

50.4.1.2. Shorewall.

Edite el archivo **/etc/shorewall/rules**:

```
vi /etc/shorewall/rules
```

Las reglas corresponderían a algo similar a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  net     fw      tcp     22
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Si la red de área local (LAN) va a acceder hacia el servidor recién configurado, es necesario abrir el puerto correspondiente.

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  net     fw      tcp     22
ACCEPT  loc     fw      tcp     22
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

O bien, hacer todo lo anterior, con una sola regla, que permita el acceso desde cualquier zona del muro cortafuegos:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  all     fw      tcp     22
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Si se decidió ofuscar el puerto de SSH, puede utilizar la siguiente regla, donde, en lugar de 52341, deberá especificar el puerto que haya elegido:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  all     fw      tcp     52341
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Al terminar de configurar las reglas para **Shorewall**, reinicie el muro cortafuegos, ejecutando el siguiente mandato:

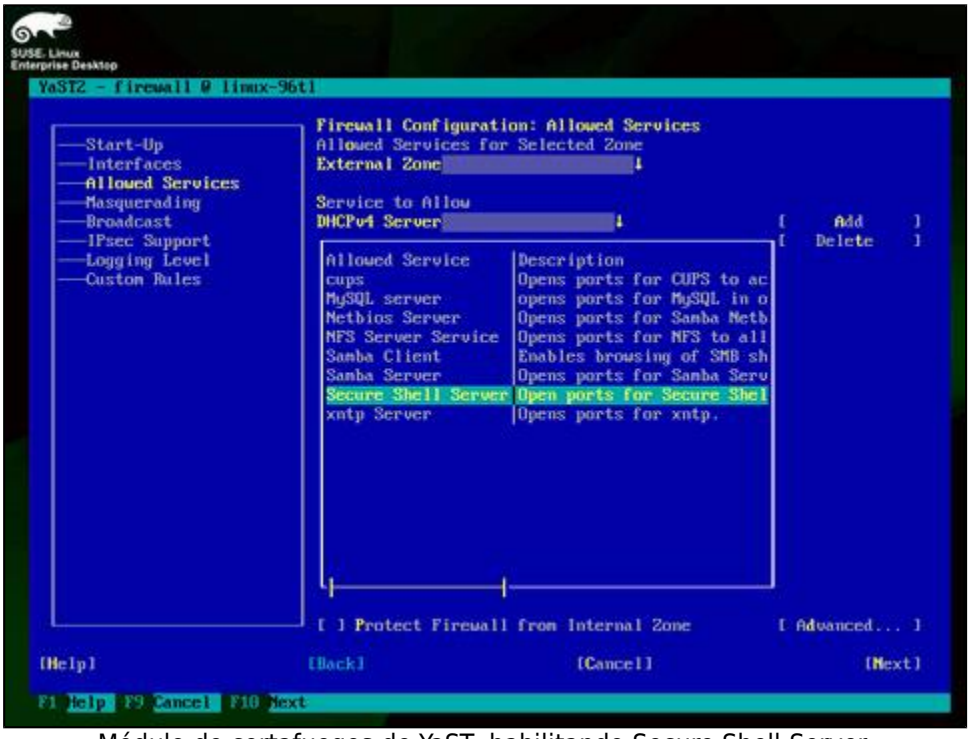
```
service shorewall restart
```

50.4.2. En openSUSE™ y SUSE™ Linux Enterprise.

Ejecute el mandato **yast** del siguiente modo:

```
yast firewall
```

Habilite **Secure Shell Server** o bien el puerto seleccionado para utilizar el servicio y aplique los cambios.



Módulo de cortafuegos de YaST, habilitando Secure Shell Server.

50.5. SELinux y el servicio sshd.

Si utiliza openSUSE™ y SUSE™ Linux Enterprise omita la siguiente sección.

Si se utiliza de **CentOS**, **Fedora™** o **Red Hat™ Enterprise Linux**, el sistema incluye tres políticas para el servicio **sshd**.

50.5.1. Política ssh_chroot_rw_homedirs.

Esta política habilita o deshabilita, la lectura y escritura de archivos a través de SFTP en los directorios de inicio de los usuarios enjaulados. El valor predeterminado es deshabilitado. Para habilitar sólo ejecute:

```
setsebool -P ssh_chroot_rw_homedirs 1
```

50.5.2. Política fenced_can_ssh.

Esta política permite a usuarios enjaulados a través de SFTP puedan ingresar también a través de SSH. El valor predeterminado es deshabilitado. Por lo general jamás se evita utilizar esta política. Para habilitar sólo ejecute:

```
setsebool -P fenced_can_ssh 1
```

50.5.3. Política ssh_chroot_manage_apache_content.

Esta política permite a usuarios enjaulados a través de SFTP puedan administrar contenido de Apache. El valor predeterminado es deshabilitado. Para habilitar sólo ejecute:

```
setsebool -P ssh_chroot_manage_apache_content 1
```

50.5.4. Política ssh_sysadm_login.

Esta política habilita o deshabilita, el acceso a través del servicio de **SSH** como administrador del sistema (contextos **sysadm_r:sysadm_t**, que corresponden a los del directorio de inicio del usuario **root** o bien que pueden ser aplicados al directorio de inicio de otro usuario con privilegios). El valor predeterminado es deshabilitado. Para habilitar sólo ejecute:

```
setsebool -P ssh_sysadm_login 1
```

50.5.5. Política allow_ssh_keysign.

Esta política habilita o deshabilita, el acceso a través de ssh utilizando firmas digitales. El valor predeterminado es deshabilitado. Para habilitar sólo ejecute:

```
setsebool -P allow_ssh_keysign 1
```

Para más detalles, consulte el documento titulado «**Cómo utilizar OpenSSH con autenticación a través de firma digital**.».

50.5.6. Contexto ssh_home_t.

El contexto de SELinux para de los directorios **~/.ssh** y sus contenidos, debe ser tipo **ssh_home_t**. En caso de haber actualizado el sistema desde versiones anteriores a CentOS 6.3 o Red Hat™ Enterprise Linux 6.3, puede re-establecer los contextos ejecutando lo siguiente:

```
restorecon -R /root
restorecon -R /home
```

O bien ejecutando:

```
chcon -R -t ssh_home_t /root/.ssh
chcon -R -t ssh_home_t /home/*/.ssh
```

50.6. Archivos de configuración.

/etc/ssh/sshd_config

Archivo principal de configuración del servidor **SSH**.

/etc/ssh/ssh_config

Archivo principal de configuración de los clientes **SSH** utilizados desde el anfitrión local.

~/.ssh/config

Archivo personal para cada usuario, que almacena la configuración utilizada por los clientes **SSH** utilizados desde el anfitrión local. Permite al usuario local utilizar una configuración distinta a la definida en el archivo **/etc/ssh/ssh_config**.

~/.ssh/known_hosts

Archivo personal para cada usuario, el cual almacena las firmas digitales de los servidores **SSH** a los que se conectan los clientes. Cuando éstas firmas cambian, se pueden actualizar utilizando el mandato **ssh-keygen** con la opción **-R** y el nombre del anfitrión como argumento, el cual elimina la entrada correspondiente del archivo **~/.ssh/known_hosts**, permitiendo añadir de nuevo el anfitrión con una nueva firma digital. Ejemplo: **ssh-keygen -R nombre.dominio.tld**.

~/.ssh/authorized_keys

Archivo personal para cada usuario, el cual almacena los certificados de los clientes **SSH**, para permitir autenticación hacia servidores **SSH** sin requerir contraseña. Consulte el documento titulado «**Cómo utilizar OpenSSH con autenticación a través de firma digital**.»

Cuando se utilizan cuentas con acceso al intérprete de mandatos, las opciones suministradas al mandato **ssh** tienen precedencia sobre las opciones establecidas en el archivo **~/.ssh/config**, que a su vez tiene precedencia sobre las opciones definidas en el archivo **/etc/ssh/ssh_config**.

50.7. Procedimientos.

Edite el archivo **/etc/ssh/sshd_config**.

```
vi /etc/ssh/sshd_config
```

A continuación se analizarán las opciones básicas que se recomienda modificar.

50.7.1. Parámetro Port.

Una forma de elevar considerablemente la seguridad al servicio de **SSH**, consiste en cambiar el número de puerto utilizado por el servicio, por otro que sólo conozca el administrador del sistema. A este tipo de técnicas se les conoce como **Seguridad por Oscuridad**. La mayoría de los delincuentes informáticos utiliza guiones que buscan servidores que respondan a peticiones a través del puerto 22. Cambiar de puerto el servicio de SSH disminuye considerablemente la posibilidad de una intrusión a través de este servicio.

```
Port 22
```

SSH trabaja a través del puerto 22 por TCP. Puede elegirse cualquier otro puerto entre el 1025 y 65535. En el siguiente ejemplo, se establecerá el puerto 52341:

```
Port 52341
```

50.7.2. Parámetro ListenAddress.

De modo predeterminado el servicio de SSH responderá peticiones a través de todas las direcciones presentes en todas las interfaces de red del sistema. En el siguiente ejemplo, el servidor a configurar tiene la dirección IP **192.168.1.254**, la cual sólo podría ser accedida desde la red local:

```
ListenAddress 192.168.1.254
```

50.7.3. Parámetro PermitRootLogin.

Establece si se va a permitir el ingreso directo del usuario root al servidor SSH. Si se va a permitir el ingreso hacia el servidor desde redes públicas, resultará prudente utilizar este parámetro con el valor **no**, de modo que sea necesario ingresar primero con una cuenta de usuario activa, con un intérprete de mandatos que permita el acceso.

```
PermitRootLogin no
```

50.7.4. Parámetro X11Forwarding.

Establece si se permitirá la ejecución remota de aplicaciones gráficas que utilicen el servidor X11. Resultará conveniente para algunas tareas administrativas que sólo puedan llevarse a cabo con herramientas gráficas o bien si se requiere utilizar una aplicación gráfica en particular. Para este fin, este parámetro puede establecerse con el valor **yes**.

```
X11Forwarding yes
```

50.7.5. Parámetro AllowUsers.

Permite restringir el acceso por usuario y/o por anfitrión. El siguiente ejemplo restringe el acceso hacia el servidor **SSH** para que sólo puedan hacerlo los usuarios fulano y mengano, desde cualquier anfitrión.

```
AllowUsers fulano mengano
```

El siguiente ejemplo restringe el acceso hacia el servidor **SSH** para que sólo puedan hacerlo los usuarios fulano y mengano, pero sólo desde los anfitriones 10.1.1.1 y 10.2.2.1.

```
AllowUsers fulano@10.1.1.1 mengano@10.1.1.1 fulano@10.2.2.1 mengano@10.2.2.1
```

50.7.6. Parámetro UseDNS.

Cuando un cliente realiza una conexión hacia un servidor SSH, éste último intentará resolver en el DNS predeterminado del sistema, la dirección IP del cliente. Si el servidor DNS predeterminado del sistema carece de una zona de resolución inversa que resuelva un nombre para la dirección IP del cliente, la conexión se demorará algunos segundos más de lo normal. Algunos administradores prefieren desactivar esta función, con el fin de agilizar las conexiones SSH en redes donde se carece de servidores DNS que tengan zonas de reenvío para resolver los nombres o zonas de resolución inversa para resolver las direcciones IP de los segmentos de red local, definiendo el valor **no** para este parámetro.

```
UseDNS no
```

Del lado del cliente se realiza un proceso de validación, que tiene como objetivo verificar si se están falsificando registros en un servidor DNS, en el caso de que éste último se haya visto comprometido en su seguridad. La opción que controla esta función es **CheckHostIP**, tiene establecido **yes** como valor predeterminado y se define en el archivo **/etc/ssh/ssh_config** (archivo de configuración para los clientes SSH del anfitrión local). Por lo general se recomienda **dejar intacta esta opción**, con el valor predeterminado, salvo que los servidores SSH involucrados carezcan de resolución en algún servidor DNS. Establecer el valor **no**, tiene como riesgo el ser susceptible de conectarse inadvertidamente a un servidor distinto al que realmente se quería utilizar, cuya resolución de nombre de anfitrión haya sido falsificada y que pudiera estar siendo utilizado con malas intenciones para engañar y poder capturar nombres de usuario y contraseñas, para posteriormente ser utilizados para acceder al servidor verdadero.

50.8. Probando OpenSSH.

50.8.1. Acceso con intérprete de mandatos.

Para acceder con intérprete de mandatos hacia el servidor, basta con ejecutar desde el sistema cliente el mandato **ssh**, definiendo como argumentos el usuario a utilizar, una arroba y la dirección IP o nombre del servidor al cual se quiera conectar:

```
ssh usuario@nombre.dominio.tld
```

Si el servidor SSH opera en un puerto diferente al 22, se puede utilizar la opción **-p** con el número de puerto utilizado como argumento. En el siguiente ejemplo, utilizando la cuenta del usuario **juan**, se intentará acceder hacia el servidor con dirección IP **192.168.70.99**, el cual tiene un servicio de **SSH** que responde peticiones a través del puerto 52341.

```
ssh -p 52341 juan@192.168.70.99
```

50.8.2. Transferencia de archivos a través de SFTP.

Para acceder a través de **SFTP** hacia el servidor, basta con ejecutar desde el sistema cliente el mandato **sftp** definiendo el usuario a utilizar y el servidor al cual conectar:

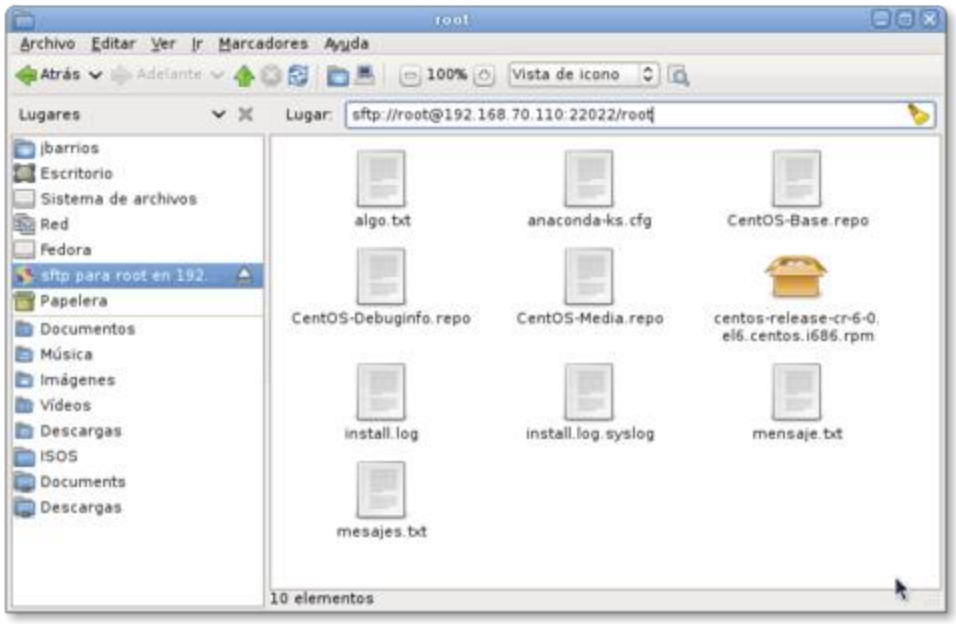
```
sftp usuario@servidor
```

El intérprete de mandatos de **SFTP** es muy similar al utilizado para el protocolo FTP y tiene las mismas funcionalidades.

Para acceder hacia un puerto en particular, en el cual está trabajando el servicio de SSH, se hace través la opción **-o** con el valor **Port=número de puerto**. En el siguiente ejemplo, utilizando la cuenta del usuario **juan**, se accederá a través de **SFTP** hacia el servidor 192.168.70.99, el cual tiene trabajando el servicio de SSH en el puerto 52341.

```
sftp -o Port=52341 juan@192.168.70.99
```

Si dispone de un escritorio en GNU/Linux, con GNOME 2.x, puede acceder hacia servidores **SSH** a través del protocolo **SFTP** utilizando el administrador de archivos (**Nautilus**) para realizar transferencias y manipulación de archivos, especificando el **URI** (**U**niform **R**esource **L**ocator o Localizador Uniforme de Recursos) **«sftp:»**, seguido del servidor y la ruta hacia la que se quiere acceder, seguido del puerto, en el caso que sea distinto al 22.



Nautilus, accediendo hacia un directorio remoto a través de **SFTP**.

50.8.2.1. Jaulas para los usuarios que acceden a través de SFTP.

La función de **chroot** (jaula de confinamiento de los usuarios) viene incluida desde la versión **4.9p1** de OpenSSH. Para habilitarla, es necesario editar el archivo /etc/ssh/sshd_config:

```
vi /etc/ssh/sshd_config
```

Casi al final del archivo, localice la siguiente línea:

```
Subsystem       sftp    /usr/libexec/openssh/sftp-server
```

Comente la línea con una almohadilla y añada el siguiente contenido:

```
#Subsystem      sftp    /usr/libexec/openssh/sftp-server
Subsystem     sftp   internal-sftp
Match Group sftpusers
    ChrootDirectory %h
    ForceCommand internal-sftp
    AllowTcpForwarding no
```

Guarde el archivo y regrese al intérprete de mandatos

Reinicie el servicio **sshd** ejecutando lo siguiente:

```
service sshd restart
```

Utilice el mandato **groupadd** para crear el grupo **sftpusers**.

```
groupadd sftpusers
```

Añada a los usuarios a los cuales se quiera enjaular, al grupo **sftpusers**.

```
gpasswd -a perengano sftpusers
```

Cambie los permisos del directorio de inicio de los usuarios involucrados, para que pertenezcan a **root** y tengan permiso de acceso 755.

```
chown root:root /home/perengano
chmod 755 /home/perengano
```

Finalmente, cambie el intérprete de mandatos de los usuarios involucrados a **/sbin/nologin**.

```
usermod -s /sbin/nologin perengano
```

A partir de este momento, los usuarios involucrados podrán ingresar al sistema a través de SFTP, pero sólo podrán tener acceso a su directorio de inicio.

```
[fulano@centos6 ~]$ sftp perengano@192.168.80.8
perengano@192.168.80.8's password:
Connected to 192.168.80.8.
sftp> pwd
Remote working directory: /
sftp> ls -a
.               ..              .bash_logout    .bash_profile   .bashrc
sftp>
```

50.8.3. Transferencia de archivos a través de SCP.

Para realizar transferencias de archivos a través de **SCP**, es necesario conocer las rutas de los directorios objetivo del anfitrión remoto. A continuación se describen algunas de las opciones más importantes del mandato **scp**.

-p (minúscula)

Preserva el tiempo de modificación, tiempos de acceso y los modos del archivo original.

-P (mayúscula)

Especifica el puerto para realizar la conexión.

-r

Copia en modo descendente de los directorios especificados.

En el siguiente ejemplo, se transferirá el archivo **algo.txt**, preservando tiempos y modos, hacia el directorio de inicio del usuario fulano en el servidor 192.169.0.99.

```
scp -p algo.txt fulano@192.168.70.99:~/
```

En el siguiente ejemplo, se transferirá la carpeta **Mail**, junto con todo su contenido, preservando tiempos y modos, **hacia** el directorio de inicio del usuario fulano en el servidor 192.169.0.99.

```
scp -rp Mail fulano@192.168.70.99:~/
```

En el siguiente ejemplo, se transferirá la carpeta **Mail**, junto con todo su contenido, **desde** el directorio de inicio del usuario fulano en el servidor 192.169.0.99, cuyo servicio de **SSH** escucha peticiones a través del puerto 52341, preservando tiempos y modos, hacia el directorio del usuario con el que se está trabajando en el anfitrión local.

```
scp -P 52341 -rp fulano@192.168.70.99:~/Mail ./
```

Por favor, continúe con el documento titulado «OpenSSH con autenticación a través de firma digital.»

51. OpenSSH con autenticación a través de firma digital.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

51.1. Introducción.

Utilizar firmas digitales en lugar de contraseñas a través de servicios como **SSH**, **SCP** o **SFTP**, resulta una técnica más segura para autenticar dichos servicios, facilitando también la operación de guiones y herramientas de respaldo que utilizan dichos protocolos.

51.2. Procedimientos

51.2.1. Modificaciones en el Servidor remoto.

Si utiliza CentOS, Fedora™ o Red Hat™ Enterprise Linux acceda como administrador al servidor remoto y habilite la política para SELinux denominada **allow_ssh_keysign**, ejecutando lo siguiente:

```
setsebool -P allow_ssh_keysign 1 && exit
```

Si utiliza openSUSE™ o SUSE™ Linux Enterprise omita el paso anterior.

Acceda nuevamente al servidor remoto pero con la cuenta de usuario que se utilizará. En el ejemplo se utilizará la misma cuenta de root.

```
ssh root@servidor
```

Si utiliza CentOS, Fedora™ o Red Hat™ Enterprise Linux ejecute los siguientes mandatos, los cuales tienen como objetivo crear el directorio **~/.ssh/** con permiso de acceso de lectura/escritura sólo para el usuario y cambiar el contexto SELinux al tipo **ssh_home_t**, crear el archivo **~/.ssh/authorized_keys** igualmente con permiso de acceso de lectura/escritura sólo para el usuario y cambiar el contexto SELinux al tipo **ssh_home_t**:

```
mkdir -m 0700 ~/.ssh/
chcon -R -t ssh_home_t ~/.ssh/
touch ~/.ssh/authorized_keys
chmod 600 ~/.ssh/authorized_keys
chcon -t ssh_home_t ~/.ssh/authorized_keys
exit
```

Si utiliza openSUSE™ o SUSE™ Linux Enterprise sólo ejecute los siguientes mandatos, los cuales tienen como objetivo crear el directorio **~/.ssh/** con permiso de acceso de lectura/escritura sólo para el usuario, crear el archivo **~/.ssh/authorized_keys** igualmente con permiso de acceso de lectura/escritura sólo para el usuario:

```
mkdir -m 0700 ~/.ssh/
touch ~/.ssh/authorized_keys
chmod 600 ~/.ssh/authorized_keys
exit
```

51.2.2. Modificaciones en el cliente.

51.2.2.1. Generar firma digital (firma digital pública).

Se debe generar una firma digital (firma digital pública) creada con **DSA** (**D**igital **S**ignature **A**lgorithm o Algoritmo de Firma digital). **Si se desea evitar utilizar contraseña para autenticar, sólo se pulsa la tecla ENTER**. Si asigna contraseña, está será utilizada para autenticar el certificado creado cada vez que se quiera utilizar éste para autenticar remotamente.

```
ssh-keygen -t dsa
```

El procedimiento devolverá una salida similar a la siguiente:

```
Generating public/private dsa key pair.
Enter file in which to save the key (/home/usuario/.ssh/id_dsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/usuario/.ssh/id_dsa.
Your public key has been saved in /home/usuario/.ssh/id_dsa.pub.
The key fingerprint is:
2c:73:30:fe:82:21:a5:52:78:49:37:cd:57:af:36:df usuario@cliente
```

Nota: Es importante resaltar que si desea utilizar la firma digital sin contraseña, jamás se deberá establecer una contraseña durante la generación de la firma digital. Cuando el diálogo de **ssh-keygen** solicite una contraseña con confirmación, sólo debe pulsar la tecla **ENTER** y continuar el procedimiento.

Lo anterior genera los archivos los archivos **~/.ssh/id_dsa** y **~/.ssh/id_dsa.pub**, los cuales deben tener permiso de acceso 600 (sólo lectura y escritura para el usuario).

```
chmod 600 ~/.ssh/{id_dsa,id_dsa.pub}
```

>Si utiliza CentOS, Fedora™ o Red Hat™ Enterprise Linux debe cambiar los contextos de **~/.ssh/** al tipo **ssh_home_t**:

```
chcon -R -t ssh_home_t ~/.ssh/
```

Si utiliza openSUSE™ o SUSE™ Linux Enterprise omita el paso anterior.

Copie el contenido del archivo correspondiente a la firma digital pública **DSA** (es decir **id_dsa.pub**) dentro del archivo **~/.ssh/authorized_keys** del usuario a utilizar en el servidor remoto. En el siguiente ejemplo se utiliza la cuenta de root del servidor remoto.

```
cat ~/.ssh/id_dsa.pub|ssh root@servidor "cat >>/root/.ssh/authorized_keys"
```

Para poder acceder al servidor desde cualquier cliente, basta copiar los archivos **id_dsa** y **id_dsa.pub** dentro del directorio **~/.ssh/**, de la cuenta de usuario de cada cliente desde el que se requiera realizar conexión hacia el servidor. Tendrá serias implicaciones de seguridad si el archivo **id_dsa** cae en manos equivocadas o se ve comprometido. **Este archivo deberá ser considerado como altamente confidencial**.

Pueden generarse diferentes firmas digitales para cada usuario que deba ingresar a través de SSH al servidor remoto. Simplemente **se añade** el contenido del archivo **~/.ssh/id_dsa.pub** de cada usuario al archivo **~/.ssh/authorized_keys** de la cuenta de usuario a utilizar en el servidor remoto. Pueden agregarse cuantas firmas digitales en este archivo como sean necesarias. Si acaso se ve comprometida la seguridad de alguna firma digital, se debe eliminar ésta del archivo **~/.ssh/authorized_keys** del servidor remoto.

51.2.3. Comprobaciones.

Si se omitió asignar contraseña para la llave **DSA**, deberá poderse acceder hacia el servidor remoto sin necesidad de autenticar con la contraseña del usuario remoto. Si fue asignada una contraseña a la clave **DSA**, se podrá acceder hacia el servidor remoto autenticando con la contraseña definida a la clave **DSA** y sin necesidad de autenticar con la contraseña del usuario remoto.

52. Configuración y uso de NTP.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

52.1. Introducción.

52.1.1. Acerca de NTP.

NTP (***N****etwork* ***T****ime* ***P****rotocol*) es un protocolo —de entre los más antiguos protocolos de Internet (1985)— utilizado para la sincronización de relojes de sistemas computacionales a través de redes, haciendo uso de intercambio de paquetes (unidades de información transportadas entre nodos a través de enlaces de datos compartidos) y latencia variable (tiempo de demora entre el momento en que algo inicia y el momento en que su efecto inicia). **NTP** fue originalmente diseñado —y sigue siendo mantenido— por Dave Mills, de la universidad de Delaware.

NTP utiliza el algoritmo de Marzullo (inventado por Keith Marzullo), el cual sirve para seleccionar fuentes de origen para la estimación exacta del tiempo a partir de un número determinado de fuentes de origen desordenadas, utilizando la escala **UTC**.

La versión 4 del protocolo puede mantener el tiempo con un margen de 10 milisegundos a través de la red mundial, alcanzado exactitud de 200 microsegundos. En redes locales, bajo condiciones idóneas, este margen se puede reducir considerablemente.

El protocolo trabaja a través del puerto 123, únicamente a través de **UDP**.

URL: http://www.ietf.org/rfc/rfc1305.txt

52.1.1.1. Estratos.

NTP utiliza el sistema jerárquico de estratos de reloj.

Estrato 0: son dispositivos, como relojes **GPS** o radio relojes, que carecen de conectividad hacia redes. Sólo están conectados a computadoras que son las encargadas de distribuir los datos.

Estrato 1: Los sistemas se sincronizan con dispositivos del estrato 0. Los sistemas de este estrato son referidos como servidores de tiempo.

Estrato 2: Los sistemas envían sus peticiones NTP hacia servidores del estrato 1, utilizando el algoritmo de Marzullo para recabar las mejores muestra de datos, descartando que parezcan proveer datos erróneos y compartiendo datos con sistemas del mismo estrato 2. Los sistemas de este estrato actúan como servidores para el estrato 3.

Estrato 3: Los sistemas utilizan funciones similares a las del estrato 2, sirviendo como servidores para el estrato 4.

Estrato 4: Los sistemas utilizan funciones similares a las del estrato 3.

Lista de servidores públicos, de estrato 1 y 2, en http://kopernix.com/?q=ntp y http://www.eecis.udel.edu/~mills/ntp/servers.html

52.1.2. Acerca de UTC.

UTC (***C****oordinated* ***U****niversal* ***T****ime* o Tiempo Universal Coordinado) es un estándar de alta precisión de tiempo atómico. Tiene segundos uniformes definidos por **TAI** (**T**iempo **A**tómico **I**nternacional o *International Atomic Time*), con segundos intercalares o adicionales que se anuncian a intervalos irregulares para compensar la desaceleración de la rotación del planeta Tierra, así como otras discrepancias. Estos segundos adicionales permiten a **UTC** estar casi a la par del Tiempo Universal (**UT** o ***U****niversal* ***T****ime*), el cual es otro estándar pero basado sobre el ángulo de rotación de la Tierra, en lugar de el paso uniforme de los segundos.

URL: http://es.wikipedia.org/wiki/UTC

52.2. Equipamiento lógico necesario.

52.2.1. En CentOS, Fedora™ y Red Hat™ Enterprise Linux.

Ejecute lo siguiente para instalar o actualizar todo necesario:

```
yum -y install ntp ntpdate
```

52.2.2. En openSUSE™ y SUSE™ Linux Enterprise.

Ejecute lo siguiente para instalar o actualizar todo necesario:

```
yast -i ntp
```

52.3. Modificaciones necesarias en el muro cortafuegos.

Es necesario abrir el acceso hacia el puerto **123** sólo por UDP (**NTP**).

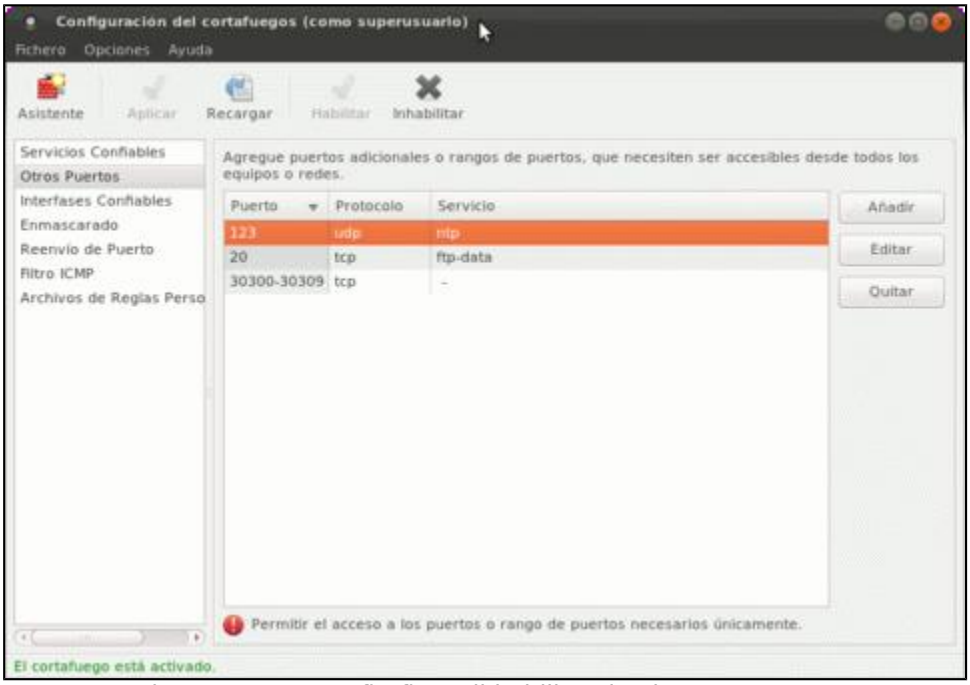
52.3.1. En CentOS, Fedora™ y Red Hat™ Enterprise Linux.

52.3.1.1. System-config-firewall.

Si utiliza el muro cortafuegos predeterminado del sistema, puede ejecutar el siguiente mandato:

```
system-config-firewall
```

Y habilite el acceso al puerto 123 por UDP y aplique los cambios.



Herramienta system-config-firewall habilitando el puerto 123 por UDP.

52.3.1.2. Servicio iptables.

Puede utilizar directamente el mandato **iptables**, ejecutando lo siguiente:

```
iptables -A INPUT -m state --state NEW -m udp -p udp --dport 123 -j ACCEPT

service iptables save
```

O bien edite el archivo **/etc/sysconfig/iptables**:

```
vim /etc/sysconfig/iptables
```

Y añada el siguiente contenido:

```
-A INPUT -m state --state NEW -m udp -p udp --dport 123 -j ACCEPT
```

Para aplicar los cambios, reinicie el servicio **iptables**:

```
service iptables restart
```

52.3.1.3. Shorewall.

Edite el archivo **/etc/shorewall/rules**:

```
vim /etc/shorewall/rules
```

Las reglas correspondería a algo similar a lo siguiente, asumiendo que sólo se va a permitir a la red de área local acceder al servidor NTP para permitir a éstos sincronizar la hora del sistema:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  loc     fw      udp     123
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Si se va a permitir a la red de área local acceder hacia servidores de tiempo localizados en Internet, en lugar de utilizar un servidor en la misma red de área local, es necesario utilizar las siguientes reglas:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  loc     net     udp     123
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Para aplicar los cambios, reinicie el servicio **shorewall**:

```
service shorewall restart
```

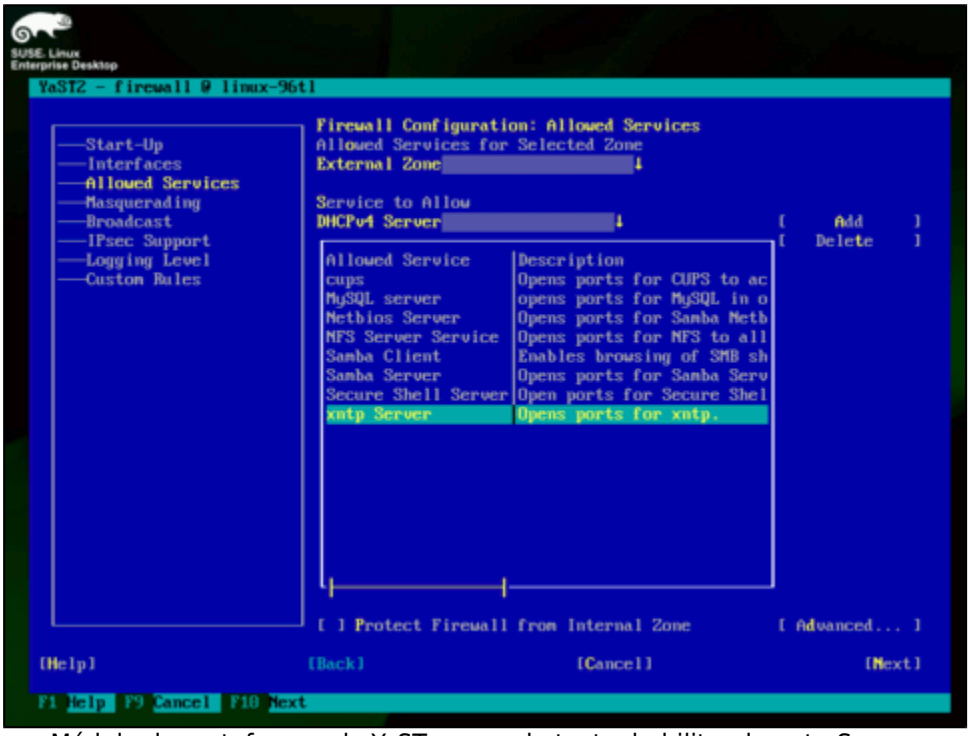
52.3.2. En openSUSE™ y SUSE™ Linux Enterprise.

Ejecute el mandato **yast** del siguiente modo:

```
yast firewall
```

Y habilite xntp Server o Servidor xntp, según sea el caso o bien abra el puerto 123 por UDP y aplique los cambios.

Módulo de cortafuegos de YaST, en modo gráfico, habilitando servidor xntp.



Módulo de cortafuegos de YaST, en modo texto, habilitando xntp Server.

52.4. Iniciar, detener y reiniciar el servicio ntpd.

52.4.1. En CentOS, Fedora™ y Red Hat™ Enterprise Linux.

El método estándar para activar o desactivar el servicio es través del mandato **chkconfig**.

Para hacer que el servicio de **ntpd** esté activo con el siguiente inicio del sistema, en todos los niveles de ejecución (2, 3, 4 y 5), se ejecuta lo siguiente:

```
chkconfig ntpd on
```

El método estándar para controlar el servicio es través del mandato **service**.

Para iniciar el servicio por primera vez, sólo necesita ejecutar:

```
service ntpd start
```

Para reiniciar el servicio sólo se necesita ejecutar:

```
service ntpd restart
```

Para detener el servicio, sólo necesita ejecutar:

```
service ntpd stop
```

52.4.2. En openSUSE™ y SUSE™ Linux Enterprise.

El método estándar para activar o desactivar el servicio es través del mandato **insserv**.

Para hacer que el servicio de **ntpd** esté activo con el siguiente inicio del sistema, en todos los niveles de ejecución (2, 3, 4 y 5), se ejecuta lo siguiente:

```
insserv ntp
```

El método estándar para controlar el servicio es través del mandato **rcntp**.

Para iniciar el servicio por primera vez, sólo necesita ejecutar:

```
rcntp start
```

Para reiniciar el servicio sólo se necesita ejecutar:

```
rcntp restart
```

Para detener el servicio, sólo necesita ejecutar:

```
rcntp stop
```

52.5. Procedimientos.

52.5.1. Herramienta ntpdate

Una forma muy sencilla de sincronizar el reloj del sistema con cualquier servidor de tiempo es a través del mandato **ntpdate**. Se trata de una herramienta similar a **rdate** y se utiliza para establecer la fecha y hora del sistema utilizando **NTP**. El siguiente ejemplo realiza una consulta directa **NTP**, utilizando el mandato **ntpdate** con la opción **-u**, para definir se utilice un puerto sin privilegios, hacia el servidor *0.pool.ntp.org*.

```
ntpdate -u 0.pool.ntp.org
```

La opción **-u** se utiliza cuando hay un cortafuegos que impide la salida desde el puerto 123/UDP o bien si el servicio **ntp** está funcionando y utilizando el puerto 123/UDP.

El manual completo del mandato **ntpdate** puede consultarse ejecutando lo siguiente:

```
man 8 ntpdate
```

52.5.2. Archivo de configuración /etc/ntp.conf.

El manual completo para el formato del archivo **/etc/ntp.conf** puede consultarse ejecutando lo siguiente:

```
man 5 ntp.conf
```

52.5.2.1. En CentOS, Fedora™ y Red Hat™ Enterprise Linux.

Los sistemas operativos como CentOS, Fedora™ y Red Hat™ Enterprise Linux, se incluye un archivo de configuración **/etc/ntp.conf**, con una configuración para uso general que permite trabajar como cliente **NTP**. Se recomienda respaldar éste para futuras consultas y utilizar un nuevo archivo en su lugar:

```
mv /etc/ntp.conf /etc/ntp.conf.original
```

Genere el nuevo archivo **/etc/ntp.conf** que permitirá funcionar como servidor **NTP** en la red de área local:

```
vim /etc/ntp.conf
```

Añada el siguiente contenido y modifique lo que considere pertinente, como serían los valores **resaltados**:

```
# Se establece la política predeterminada para cualquier
# servidor de tiempo utilizado: se permite la sincronización
# de tiempo con las fuentes, pero sin permitir a la fuente
# consultar (noquery), ni modificar el servicio en el
# sistema (nomodify) y declinando proveer mensajes de
# registro (notrap).
restrict default nomodify notrap noquery
restrict -6 default nomodify notrap noquery

# Permitir todo el acceso a la interfaz de retorno del
# sistema.
restrict 127.0.0.1
restrict -6 ::1

# Se le permite a las redes local sincronizar con el servidor
# pero sin permitirles modificar la configuración del
# sistema y sin usar a éstos como iguales para sincronizar.
# Cambiar por las que correspondan a sus propias redes locales.
restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap
restrict 192.168.70.0 mask 255.255.255.128 nomodify notrap
restrict 172.16.1.0 mask 255.255.255.240 nomodify notrap
restrict 10.0.1.0 mask 255.255.255.248 nomodify notrap

# Reloj local indisciplinado.
# Este es un controlador emulado que se utiliza sólo como
# respaldo cuando ninguna de las fuentes reales están
# disponibles.
fudge   127.127.1.0 stratum 10
server  127.127.1.0

# Archivo de variaciones.
driftfile /var/lib/ntp/drift
broadcastdelay  0.008

# Archivo de claves si acaso fuesen necesarias para realizar
# consultas
keys            /etc/ntp/keys

# Lista de servidores de tiempo de estrato 1 o 2.
# Se recomienda tener al menos 3 servidores listados.
# Mas servidores en:
#               http://kopernix.com/?q=ntp
#               http://www.eecis.udel.edu/~mills/ntp/servers.html
server 0.pool.ntp.org iburst
server 1.pool.ntp.org iburst
server 2.pool.ntp.org iburst
server 3.pool.ntp.org iburst

# Permisos que se asignarán para cada servidor de tiempo.
# En los ejemplos, se impide a las fuente consultar o modificar
# el servicio en el sistema, así como también enviar mensaje de
# registro.
restrict 0.pool.ntp.org mask 255.255.255.255 nomodify notrap noquery
restrict 1.pool.ntp.org mask 255.255.255.255 nomodify notrap noquery
restrict 2.pool.ntp.org mask 255.255.255.255 nomodify notrap noquery
restrict 3.pool.ntp.org mask 255.255.255.255 nomodify notrap noquery

# Se activa la difusión hacia los clientes
broadcastclient
```

Para aplicar los cambios, ejecute lo siguiente:

```
service ntpd restart
```

Para sincronizar la hora de inmediato en este servidor recién configurado, ejecute:

```
ntpdate -u 0.pool.ntp.org
```

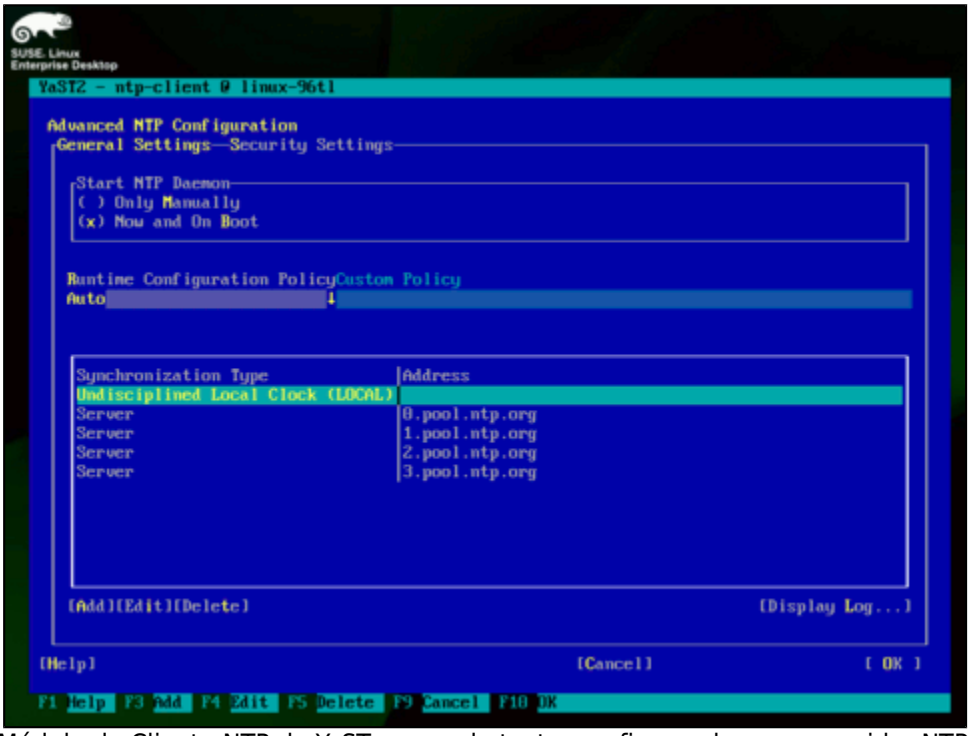
52.5.2.2. En openSUSE™ y SUSE™ Linux Enterprise.

Evite modificar directamente el archivo **/etc/ntpd.conf**, pues el método preferido de configuración es a través del módulo correspondiente de **YaST**. En su lugar utilice el módulo Cliente NTP de YaST, ejecutando lo siguiente:

```
yast ntp-client
```

Conserve el reloj local indisciplinado, defina los servidores NTP a utilizar y aplique los cambios.

Módulo de Cliente NTP de YaST, en modo gráfico, configurando como servidor NTP.



Módulo de Cliente NTP de YaST, en modo texto, configurando como servidor NTP.

Para sincronizar la hora de inmediato en este servidor recién configurado, ejecute:

```
ntpdate -u 0.pool.ntp.org
```

52.5.3. Configuración de clientes.

Asumiendo que los clientes GNU/Linux ya tiene instalados los paquetes de NTP y que el servidor tiene una dirección IP 172.16.1.1, verifique primero que hay conectividad hacia el nuevo servidor que acaba de configurar ejecutando como root lo siguiente:

```
ntpdate -u 172.16.1.1
```

Lo anterior debe devolver una salida similar a la siguiente:

```
18 Sep 13:30:15 ntpdate[4913]: adjust time server 172.16.1.1 offset -0.000812 sec
```

Si lo anterior falla, verifique la configuración en el servidor y su muro cortafuegos.

52.5.3.1. Asignación automática a través de servidor DHCP.

La forma más simple y práctica de replicar automáticamente la asignación de servidores NTP en la red de área local, es a través de un servidor DHCP.

Edite el archivo **/etc/dhcp/dhcpd.conf** o **/etc/dhcpd.conf**, de acuerdo a la versión de sistema operativo utilizado:

```
vim /etc/dhcp/dhcpd.conf
```

Utilice la opción **ntp-servers** para definir una lista separada por comas de todos los servidores NTP que se quiera utilizar en la red de área local:

```
ddns-update-style interim;
ignore client-updates;
authoritative;
default-lease-time 900;
max-lease-time 7200;
option ip-forwarding off;
option domain-name "red-local.net";
option ntp-servers 172.16.1.1;

shared-network redlocal {
        subnet 172.16.1.0 netmask 255.255.255.192 {
                option routers 172.16.1.1;
                option subnet-mask 255.255.255.192;
                option broadcast-address 172.16.1.63;
                option domain-name-servers 172.16.1.1;
                option netbios-name-servers 172.16.1.1;
                range 172.16.1.2 172.16.1.58;
        }
}
```

Reinicie el servicio **dhcpd** a fin de que surtan efecto los cambios.

```
service dhcpd restart
```

Para más detalles acerca de la configuración de servidor DHCP, por favor consulte el documento titulado «*Configuración de servidor DHCP*.»

52.5.3.2. Configuración manual en CentOS, Fedora™ y Red Hat™ Enterprise Linux.

Edite el archivo **/etc/ntpd.conf**:

```
vim /etc/ntp.conf
```

Añada o modifique el siguiente contenido:

```
driftfile /var/lib/ntp/drift
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
restrict 127.0.0.1
restrict -6 ::1
server 172.16.1.1 iburst
includefile /etc/ntp/crypto/pw
keys /etc/ntp/keys
```

Y reinicie el servicio **ntp** a fin de que surtan efecto los cambios:

```
service ntpd restart
```

52.5.3.3. Configuración manual en openSUSE™ y SUSE™ Linux Enterprise.

Evite modificar archivo **/etc/ntpd.conf**, pues el método preferido de configuración es a través de YaST.

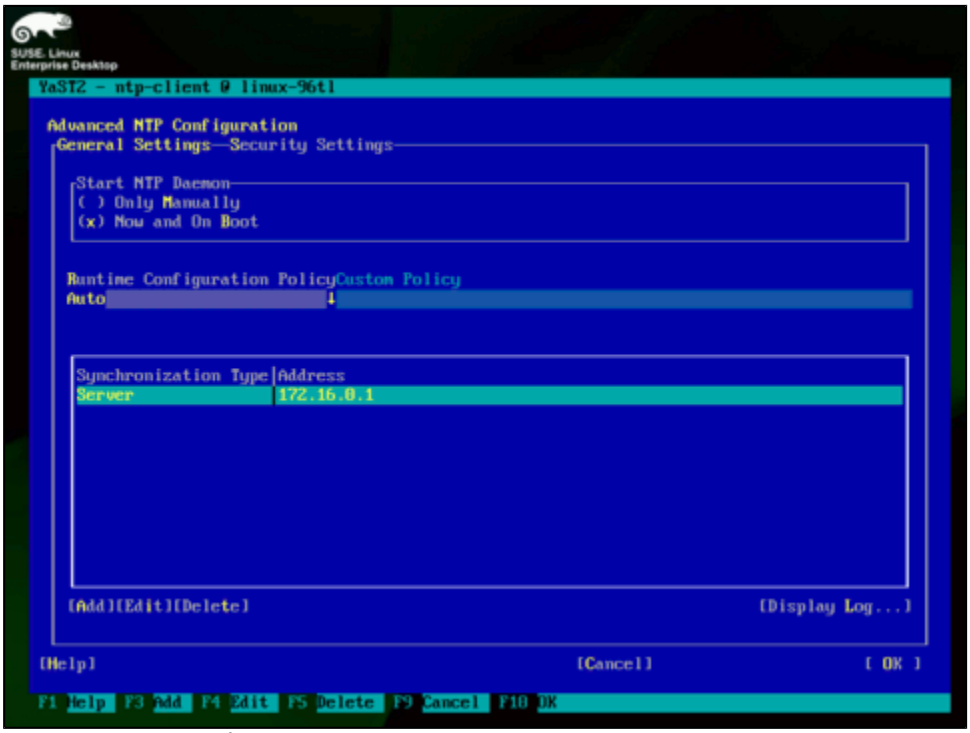
```
vim /etc/ntp.conf
```

Utilice el módulo Cliente NTP de YaST, ejecutando lo siguiente:

```
yast ntp-client
```

Elimine el reloj local indisciplinado, defina el servidor NTP a utilizar y aplique los cambios.

Módulo de Cliente NTP de YaST, en modo gráfico.



Módulo de Cliente NTP de YaST, en modo texto.

53. Configuración de servidor NFS.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

53.1. Introducción.

NFS (**N**etwork **F**ile **S**ystem), es un popular protocolo utilizado para compartir sistemas de archivos de manera transparente entre anfitriones dentro de una red de área local. Es utilizado para sistemas de archivos distribuido.

Fue desarrollado en 1984 por Sun Microsystems, teniendo en mente la independencia del anfitrión, sistema operativo, protocolo de transporte. Funciona a través de los protocolos **XDR** (nivel de presentación del modelo OSI de TCP/IP) y **ONC RPC** (nivel de sesión del modelo OSI de TCP/IP).

Es muy popular entre sistemas basados sobre el estándar POSIX y viene incluido en la mayoría de éstos de modo predeterminado. Es muy fácil de configurar y utilizar, sin embargo cabe señalar que hay quienes denominan *cariñosamente* a **NFS** como "*No File Security*", pues carece de soporte para validar usuarios por contraseñas, como lo hacen otras alternativas como Samba. Su seguridad se basa sobre listas de de control de acceso compuestas por direcciones IP o nombres de anfitrión. Es por ésto que es importante que el administrador de la red de área local comprenda que un servidor NFS puede ser un serio problema de seguridad, si éste es configurado incorrectamente.

Existen tres versiones de NFS que se utilizan hoy en día:

- **NFSv2**: Es la versión más antigua y mejor soportada.
- **NFSv3**: Tiene más características que NFSv2, como el manejo de archivos de tamaño variable y mejores informes de errores. Sólo es parcialmente compatible con los clientes para NFSv2.
- **NFSv4**: Es la versión más moderna, y, entre otras cosas, incluye soporte para seguridad a través de Kerberos, soporte para ACL y utiliza operaciones con descripción del estado.

Salvo que se trate de directorios de acceso público, se recomienda utilizar **NFS** sólo dentro de una red de área local detrás de un muro contrafuegos y que sólo se permita el acceso a los anfitriones que integren la red de área local y evitar compartir sistemas de archivos con información sensible a través de Internet.

53.2. Equipamiento lógico necesario.

53.2.1. En CentOS, Fedora y Red Hat Enterprise Linux.

El paquete **nfs-utils** viene incluido junto con la instalación estándar de estos sistemas operativos y contiene tanto las herramientas de cliente como las de servidor. De ser necesario, como por ejemplo en el caso de una instalación mínima, ejecute lo siguiente para instalar todo lo necesario:

```
yum -y install nfs-utils
```

Si prefiere una herramienta gráfica para configurar el servidor NFS, puede instalar también el paquete **system-config-nfs**:

```
yum -y install system-config-nfs
```

53.2.2. Instalación en openSUSE y SUSE Linux Enterprise.

En estos sistemas operativos, existen dos paquetes a instalar: **nfs-client**, que corresponde a las herramientas para clientes NFS y **nfs-kernel-server**, que corresponde a las herramientas de servidor NFS. Ambos paquetes están incluidos en la instalación estándar de openSUSE y SUSE Linux Enterprise. En caso de haber hecho una instalación mínima, ejecute lo siguiente para instalarlos:

```
yast -i nfs-client nfs-kernel-server
```

Si prefiere una herramienta, que funciona tanto desde la terminal como desde el escritorio, para configurar el sistema como cliente NFS, puede instalar también el paquete **yast2-nfs-client**.

```
yast -i yast2-nfs-client
```

Si prefiere una herramienta, que funciona tanto desde la terminal como desde el escritorio, para configurar el sistema como servidor NFS, puede instalar también el paquete **yast2-nfs-server**.

```
yast -i yast2-nfs-server
```

53.3. Definir los puertos utilizados por NFS.

El siguiente paso puede ser omitido en openSUSE y SUSE Linux Enterprise, gracias a que **SuSEFirewall2** detecta automáticamente los puertos aleatorios utilizados por el servicio **nfsserver**.

En CentOS, Fedora y Red Hat Enterprise Linux es importante definir los puertos fijos que utilizará NFS, pues el cortafuegos es incapaz de abrir dinámicamente los puertos aleatorios que de modo predeterminado utiliza éste.

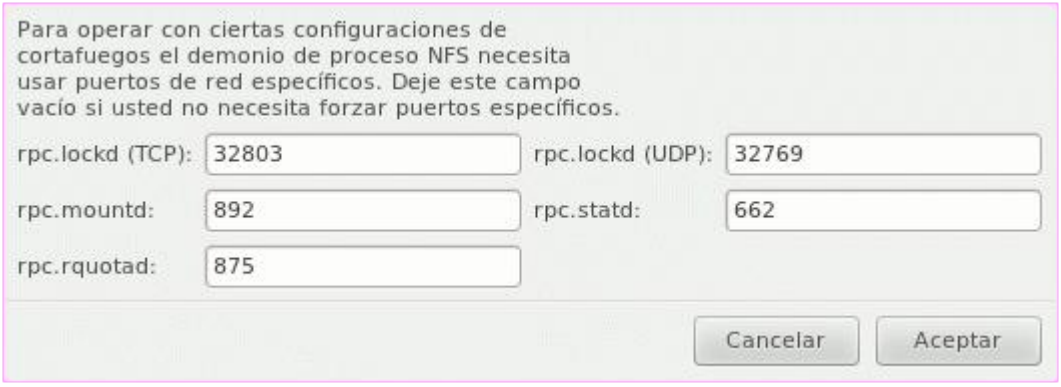
Edite el archivo **/etc/sysconfig/nfs**:

```
vi /etc/sysconfig/nfs
```

Habilite o bien modifique, los siguientes parámetros, estableciendo los valores mostrados a continuación:

```
RQUOTAD_PORT=875
LOCKD_TCPPORT=32803
LOCKD_UDPPORT=32769
MOUNTD_PORT=892
STATD_PORT=662
```

También puede establecer los puertos desde la ventana «Configuración de servidor» de la herramienta **system-config-nfs**.



Configuración del Servidor en **system-config-nfs**.

Si el servidor NFS va a trabajar sin muro cortafuegos en una red de área local, este paso es innecesario.

53.4. Iniciar servicio y añadir el servicio al inicio del sistema.

53.4.1. En CentOS, Fedora y Red Hat Enterprise Linux.

Si se realizó una instalación estándar, los servicios requeridos por **nfs**, es decir **rpcbind** y **nfslock**, estarán activos y funcionando. Sólo en el caso de haber realizado una instalación mínima, es necesario iniciar primero estos dos servicios, ejecutando lo siguiente:

```
service rpcbind start
service nfslock start
```

De modo predeterminado los servicios **rpcbind** y **nfslock** estarán activos en los niveles de ejecución 3, 4 y 5.

De modo predeterminado el servicio **nfs** estará inactivo. Para activar este servicio en los niveles de ejecución 3 y 5, es decir los niveles recomendados, ejecute lo siguiente:

```
chkconfig --level 35 nfs on
```

El método estándar para detener, iniciar o reiniciar el servicio **nfs**, es través del mandato **service**, el nombre del servicio (**nfs**) y reload, restart, start o stop como argumentos.

Para iniciar el servicio por primera vez, sólo necesita ejecutar:

```
service nfs start
```

Para volver a leer la configuración del servicio y aplicar los cambios, sin interrumpir las conexiones existentes, sólo se necesita ejecutar:

```
service nfs reload
```

Para reiniciar el servicio sólo se necesita ejecutar:

```
service nfs restart
```

Para detener el servicio, sólo necesita ejecutar:

```
service nfs stop
```

Para verificar el estado del servicio, sólo necesita ejecutar:

```
service nfs status
```

53.4.2. En openSUSE y SUSE Linux Enterprise.

El método estándar para agregar el servicio al inicio del sistema es a través del mandato **insserv**. Para activar el servicio en los niveles de ejecución 3 y 5, ejecute lo siguiente:

```
insserv nfsserver
```

El método estándar para detener, iniciar o reiniciar el servicio, es través del mandato **rcnfsserver**.

Para iniciar el servicio por primera vez, sólo necesita ejecutar:

```
rcnfsserver start
```

Para volver a leer la configuración del servicio y aplicar los cambios, sin interrumpir las conexiones existentes, sólo se necesita ejecutar:

```
rcnfsserver reload
```

Para reiniciar el servicio sólo se necesita ejecutar:

```
rcnfsserver restart
```

Para detener el servicio, sólo necesita ejecutar:

```
rcnfsserver stop
```

Para verificar el estado del servicio, sólo necesita ejecutar:

```
rcnfsserver status
```

53.5. Modificaciones necesarias en los archivos /etc/hosts.allow y /etc/hosts.deny.

Conviene establecer un poco de seguridad extra a través de **tcp_wrapper** (**tcpd**), sobre todo si el servidor NFS sólo va a operar en una red de área local sin muro cortafuegos.

Edite el archivo **/etc/hosts.deny**:

```
vi /etc/hosts.deny
```

Añada el siguiente contenido:

```
portmap: ALL
lockd: ALL
mountd: ALL
rquotad: ALL
statd: ALL
```

Edite el archivo **/etc/hosts.allow**:

```
vi /etc/hosts.allow
```

Asumiendo que se va a permitir el acceso a las redes **192.168.70.0/25**, **172.16.1.0/28** y **10.0.1.0/29**, añada el siguiente contenido:

```
portmap: 192.168.70.0/25, 172.16.1.0/28, 10.0.1.0/29
lockd: 192.168.70.0/25, 172.16.1.0/28, 10.0.1.0/29
mountd: 192.168.70.0/25, 172.16.1.0/28, 10.0.1.0/29
rquotad: 192.168.70.0/25, 172.16.1.0/28, 10.0.1.0/29
statd: 192.168.70.0/25, 172.16.1.0/28, 10.0.1.0/29
```

Los cambios aplican de manera inmediata, sin reiniciar servicio alguno.

53.6. Modificaciones necesarias en el muro cortafuegos.

verifique ejecutando el mandato **rpcinfo** con la opción **-p** los puertos y protocolos utilizados por los servicios **portmapper**, **nfs**, **lockd**, **mountd**, **rquotad** y **statd**.

```
rpcinfo -p
```

La salida debe ser similar a la siguiente.

```
   program vers proto   port  service
    100000    4   tcp    111  portmapper
    100000    3   tcp    111  portmapper
    100000    2   tcp    111  portmapper
    100000    4   udp    111  portmapper
    100000    3   udp    111  portmapper
    100000    2   udp    111  portmapper
    100011    1   udp    875  rquotad
    100011    2   udp    875  rquotad
    100011    1   tcp    875  rquotad
    100011    2   tcp    875  rquotad
    100003    2   tcp   2049  nfs
    100003    3   tcp   2049  nfs
    100003    4   tcp   2049  nfs
    100227    2   tcp   2049  nfs_acl
    100227    3   tcp   2049  nfs_acl
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100003    4   udp   2049  nfs
    100227    2   udp   2049  nfs_acl
    100227    3   udp   2049  nfs_acl
    100021    1   udp  32769  nlockmgr
    100021    3   udp  32769  nlockmgr
    100021    4   udp  32769  nlockmgr
    100021    1   tcp  32803  nlockmgr
    100021    3   tcp  32803  nlockmgr
    100021    4   tcp  32803  nlockmgr
    100005    1   udp    892  mountd
    100005    1   tcp    892  mountd
    100005    2   udp    892  mountd
    100005    2   tcp    892  mountd
    100005    3   udp    892  mountd
    100005    3   tcp    892  mountd
```

Para servidores de NFSv4, en realidad sólo es necesario abrir en el muro cortafuegos el puerto **2049/TCP** (**nfs**), pues es esta versión dejó de depender del servicio de mapa de puertos (portmap). Sin embargo, para poder trabajar con compatibilidad para NFSv2 y NFSv3, es necesario abrir los puertos **111/UDP**, **111/TCP**, **662/TCP**, **662/UDP**, **875/TCP**, **875/UDP**, **892/TCP**, **892/UDP**, **2029/TCP**, **2049/UDP**, **32803/TCP** y **32769/UDP**. Los puertos que se abran para los servicios **lockd**, **mountd**, **rquotad** y **statd** deben corresponder con los mismo puertos definidos el archivo **/etc/sysconfig/nfs**.

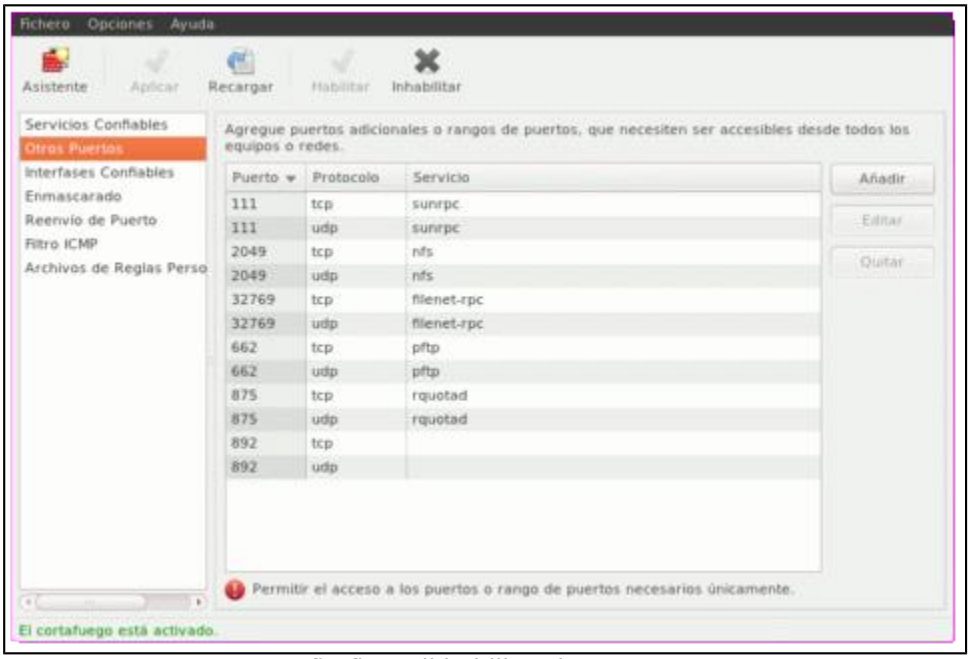
53.6.1. En CentOS, Fedora y Red Hat Enterprise Linux.

53.6.1.1. Herramienta system-config-firewall.

Si utiliza el muro cortafuegos predeterminado del sistema, puede ejecutar el siguiente mandato:

```
system-config-firewall
```

Habilite los puertos **111/UDP**, **111/TCP**, **662/TCP**, **662/UDP**, **875/TCP**, **875/UDP**, **892/TCP**, **892/UDP**, **2029/TCP**, **2049/UDP**, **32803/TCP** y **32769/UDP** y aplique los cambios.



System-config-firewall habilitando puertos para NFS.

53.6.1.2. Servicio iptables.

Si lo prefiere, también puede utilizar directamente el mandato **iptables**, ejecutando lo siguiente:

```
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 2049 -j ACCEPT
iptables -A INPUT -m state --state NEW -m udp -p udp --dport 2049 -j ACCEPT
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 111 -j ACCEPT
iptables -A INPUT -m state --state NEW -m udp -p udp --dport 111 -j ACCEPT
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 662 -j ACCEPT
iptables -A INPUT -m state --state NEW -m udp -p udp --dport 662 -j ACCEPT
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 875 -j ACCEPT
iptables -A INPUT -m state --state NEW -m udp -p udp --dport 875 -j ACCEPT
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 892 -j ACCEPT
iptables -A INPUT -m state --state NEW -m udp -p udp --dport 892 -j ACCEPT
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 32803 -j ACCEPT
iptables -A INPUT -m state --state NEW -m udp -p udp --dport 32769 -j ACCEPT

service iptables save
```

O bien añada lo siguiente al archivo **/etc/sysconfig/iptables**:

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 2049 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 2049 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 111 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 111 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 662 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 662 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 875 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 875 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 892 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 892 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 32803 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 32769 -j ACCEPT
```

Y reinicie el servicio **iptables**:

```
service iptables restart
```

53.6.1.3. Shorewall.

Las reglas para el archivo **/etc/shorewall/rules** de **Shorewall** corresponderían a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  all     fw      tcp     111,662,875,892,2049,32803
ACCEPT  all     fw      udp     111,662,875,892,2049,32769
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Para aplicar los cambios en Shorewall, ejecute lo siguiente:

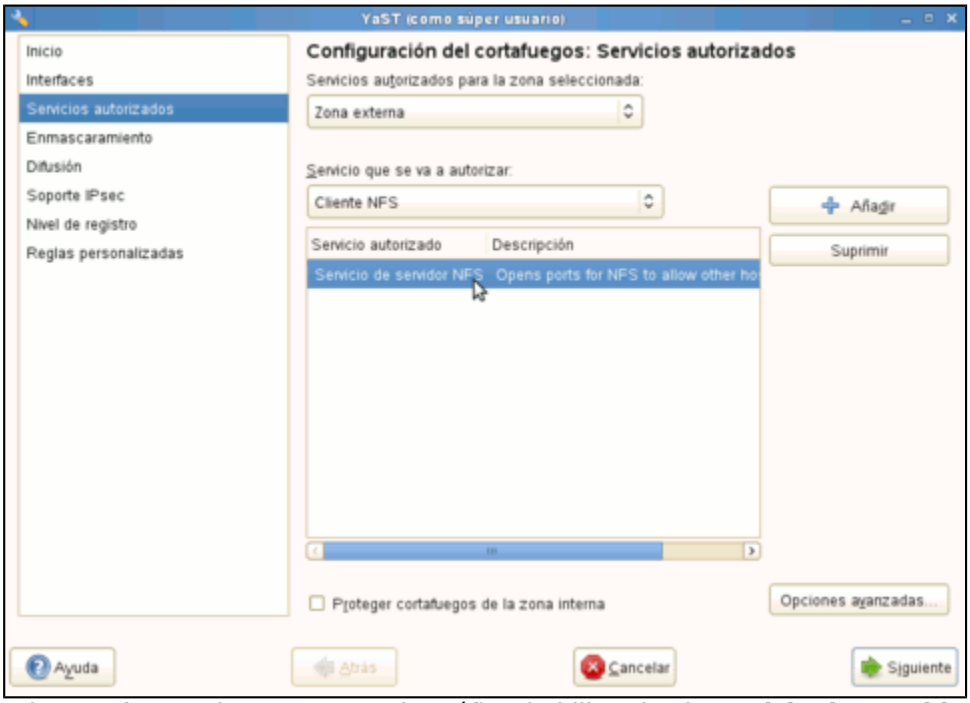
```
service shorewall restart
```

53.6.2. En openSUSE y SUSE Linux Enterprise.

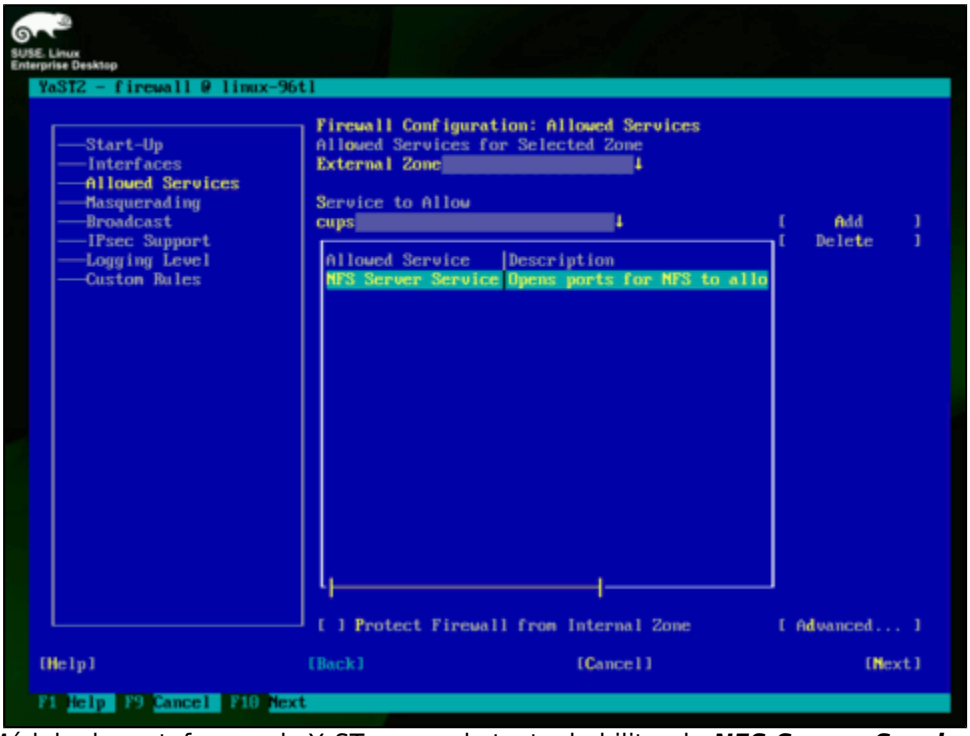
Ejecute el mandato **yast** del siguiente modo:

```
yast firewall
```

Y habilite ***NFS Server Service*** o ***Servicio de Servidor NFS*** y aplique los cambios. Ésto habilitará todos los puertos necesarios.



Módulo de cortafuegos de YaST, en modo gráfico, habilitando el ***Servicio de Servidor NFS***.



Módulo de cortafuegos de YaST, en modo texto, habilitando ***NFS Server Service***.

53.7. Procedimientos.

53.7.1. El archivo /etc/exports.

Es el archivo utilizado para configurar los directorios que se compartirán a través de NFS. El formato utilizado es el siguiente:

```
/directorio/a/compatir  anfitriones(opciones)
```

Se puede compartir cualquier directorio del sistema y sus respectivos subdirectorios, excepto por aquellos subdirectorios que estén en otros sistemas de archivos.

Los anfitriones se pueden definir por dominios, nombres de anfitrión, direcciones IP o segmentos de bloques de direcciones IP.

Las opciones utilizadas pueden ser las siguientes:

- **ro** y **rw**: Sólo lectura o lectura y escritura, respectivamente. Valor predeterminado es **rw**.
- **link_relative** y **link_absolute**: convertir los enlaces simbólicos absolutos en enlaces simbólicos relativos o bien dejar los enlaces simbólicos como están, respectivamente. Valor predeterminado es link_absolute.
- **no_root_squash** y **root_squash**: respeta el uid/gid 0 (root) o bien traslada uid/gid 0 hacia uid/gid del usuario anónimo de NFS. Valor predeterminado es root_squash.
- **squash_uids** y **squash_gids**: especifica una lista de uids o gids que se trasladarán al usuario anónimo utilizado por NFS. Ejemplo: squash_uids=0-15,20,25-50.

- **all_squash**: traslada todos los uid y gid hacia el uid y gid del usuario anónimo utilizado por NFS. Comúnmente utilizado para compartir directorios de acceso público, como el directorio **/var/ftp/pub**.

- **anonuid** y **anongid**: establecen en forma explícita el uid y gid del usuario anónimo utilizado por NFS. Ejemplo: anonuid=150,anongid=100.

El manual que detalla el formato y opciones del archivo **/etc/exports** puede consultarse ejecutando lo siguiente:

```
man 5 exports
```

Para ver la lista de clientes conectados al servidor NFS, se ejecuta el mandato **showmount**:

```
showmount
```

Para ver la lista de clientes conectados al servidor NFS y los directorios utilizados por cada uno, se ejecuta el mandato **showmount** con la opción **-a**:

```
showmount -a
```

El manual que detalla las opciones del mandato **showmount** puede consultarse ejecutando lo siguiente:

```
man 8 showmount
```

53.7.1.1. Ejemplos de configuración del archivo /etc/exports.

En el siguiente ejemplo, se comparte el directorio local **/home** en modo **lectura y escritura** (**rw**) a todos los anfitriones de **172.16.1.0/28**, respetando el uid y gid de root (**no_root_squash**):

```
/home   172.16.1.0/28(rw,no_root_squash)
```

En el siguiente ejemplo, se comparte el directorio local **/var/www** en modo **lectura y escritura** (**rw**) a **172.16.1.2**, respetando el uid y gid de root (**no_root_squash**) y a **172.16.1.3** en modo de **sólo lectura**, trasladando todos los uid y gid al usuario anónimo utilizado por NFS (**root_squash** es el valor por omisión):

```
/var/www        172.16.1.2(rw,no_root_squash)   172.16.1.3(ro,all_squash)
```

53.7.1.2. Herramienta system-config-nfs en CentOS, Fedora y Red Hat Enterprise Linux.

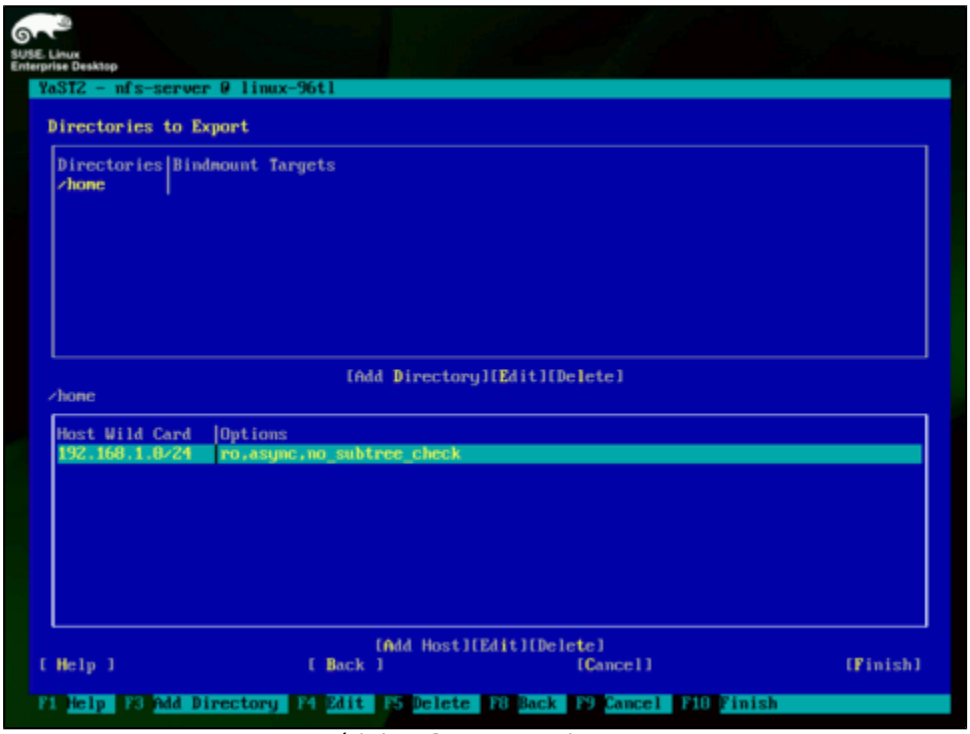
La configuración de los directorios a exportar, con sus posibles opciones, en el archivo **/etc/exports**, así como la configuración de los puertos de NFS en el archivo **/etc/sysconfig/nfs**, pueden hacer desde la herramienta gráfica **system-config-nfs**.

Herramienta gráfica **system-config-nfs**.

53.7.1.3. YaST nfs-server en openSUSE y SUSE Linux Enterprise.

La configuración de los directorios a exportar, con sus posibles opciones, en el archivo **/etc/exports**, así como la configuración de opciones del servidor NFS, pueden hacer utilizando el módulo **nfs-server** de YaST. Ejecute lo siguiente:

```
yast nfs-server
```



Módulo **nfs-server** de YaST.

53.7.2. Verificación del servicio.

El mandato **rpcinfo** se utiliza para verificar el estado de servidores NFS y otros servidores que funcionan sobre RPC.

Para verificar el estado de los servicios en el anfitrión local, ejecute:

```
rpcinfo
```

Para ver las estadísticas de uso en el anfitrión local, ejecute el mandato **rpcinfo** con la opción **-m**:

```
rpcinfo -m
```

Para mostrar una lista de todos los programas RPC en el anfitrión local, ejecute el mandato **rpcinfo** con la opción **-p**:

```
rpcinfo -p
```

Para mostrar una lista más concisa de todos los programas RPC en el anfitrión local, ejecute el mandato **rpcinfo** con la opción **-s**:

```
rpcinfo -s
```

Para mostrar los transportes soportados por el anfitrión local, ejecute el mandato **rpcinfo** con la opción **-T**, **udp**, el nombre o dirección IP del anfitrión local y **nfs** como argumentos. Ejemplo:

```
rpcinfo -T udp localhost nfs
```

Para verificar el estado de los servicios en un anfitrión remoto, ejecute el mandato **rpcinfo** con el nombre o dirección IP de un servidor NFS remoto como argumento. Ejemplo:

```
rpcinfo 192.168.1.64
```

Para ver las estadísticas de uso en un anfitrión remoto, ejecute el mandato **rpcinfo** con la opción **-m** y el nombre o dirección IP de un servidor NFS remoto como argumento. Ejemplo:

```
rpcinfo -m 192.168.1.64
```

Para mostrar una lista de todos los programas RPC en un anfitrión remoto, ejecute el mandato **rpcinfo** con la opción **-p** y el nombre o dirección IP de un servidor NFS remoto como argumento. Ejemplo:

```
rpcinfo -p 192.168.1.64
```

Para mostrar una lista más concisa de todos los programas RPC en un anfitrión remoto, ejecute el mandato **rpcinfo** con la opción **-s** y el nombre o dirección IP de un servidor NFS remoto como argumento. Ejemplo:

```
rpcinfo -s 192.168.1.64
```

Para mostrar los transportes soportados por un anfitrión remoto, ejecute el mandato **rpcinfo** con la opción **-T**, **udp**, el nombre o dirección IP de un servidor NFS remoto y **nfs** como argumentos. Ejemplo:

```
rpcinfo -T udp 192.168.1.64 nfs
```

53.7.3. Montaje de sistemas de archivos NFS.

Para montar sistemas de archivos tipo NFS se utiliza el mandato **mount** con la siguiente sintaxis:

```
mount [-o opciones] servidor:/directorio /punto/montaje
```

Para hacer permanentes los puntos de montaje, se añaden entradas en el archivo **/etc/fstab**, utilizando el siguiente formato:

```
servidor:/directorio   /punto/montaje   nfs4   opciones  0 0
```

Las posibles opciones para ambos archivos, son las siguientes:

- **rsize**: Define el tamaño del búfer para lectura. El valor predeterminado es 1024 bytes. Si se incrementa a 8192 bytes, mejora considerablemente el rendimiento del servidor NFS al hacer la lectura de datos desde el cliente. Ejemplo: mount -o rsize=8192 servidor:/directorio /mnt/servidor

- **wsize**: Define el tamaño del búfer para escrituras. El valor predeterminado es 1024 bytes. Si se incrementa a 8192 bytes, mejora considerablemente el rendimiento del servidor NFS al hacer la escritura de datos desde el cliente. Ejemplo: mount -o wsize=8192 servidor:/directorio /mnt/servidor

- **hard** y **soft**: El primero hace que las aplicaciones que estén utilizando el sistema de archivos remoto entren en pausa cuando falle o se interrumpa la conectividad con el servidor NFS, pudiendo utilizarse en combinación con la opción intr para poder interrumpir las aplicaciones pausadas. El segundo permite, después de un tiempo que se define con la opción timeo, descartar las conexiones fallidas o interrumpidas hacia un servidor NFS.

- **intr**: Permite interrumpir las aplicaciones y/o los procesos que hayan sido pausados tras la falla o interrupción de conectividad con un servidor NFS.

- **timeo**: Se utiliza para establecer el límite de tiempo en décimas de segundo usado antes de la primera retransmisión después de que ha fallado o se ha interrumpido una conexión a un servidor NFS. El valor por omisión es 7 décimas de segundo, tras lo cual se duplica por cada expiración RPC, hasta un máximo de 60 segundos. Se recomienda aumentar el valor en redes con mucha congestión.

- **auto** y **noauto**: El primero define si el sistema de archivos remoto se montará automáticamente junto con el inicio del sistema. El segundo impide que se monte automáticamente el sistema de archivos remoto. El valor predeterminado es **auto**.

- **user**: permite a los usuarios regulares poder montar un sistema de archivos NFS. Automáticamente añade las opciones **noexec**, **nosuid** y **nodev** (prohibido ejecutar archivos de este sistema de archivos, prohibido utilizar SUID, prohibido el uso de dispositivos de bloque, respectivamente).

El manual que detalla las opciones de montado para NFS para el archivo **/etc/fstab** y que también son utilizadas por el mandato **mount**, pueden consultarse ejecutando lo siguiente:

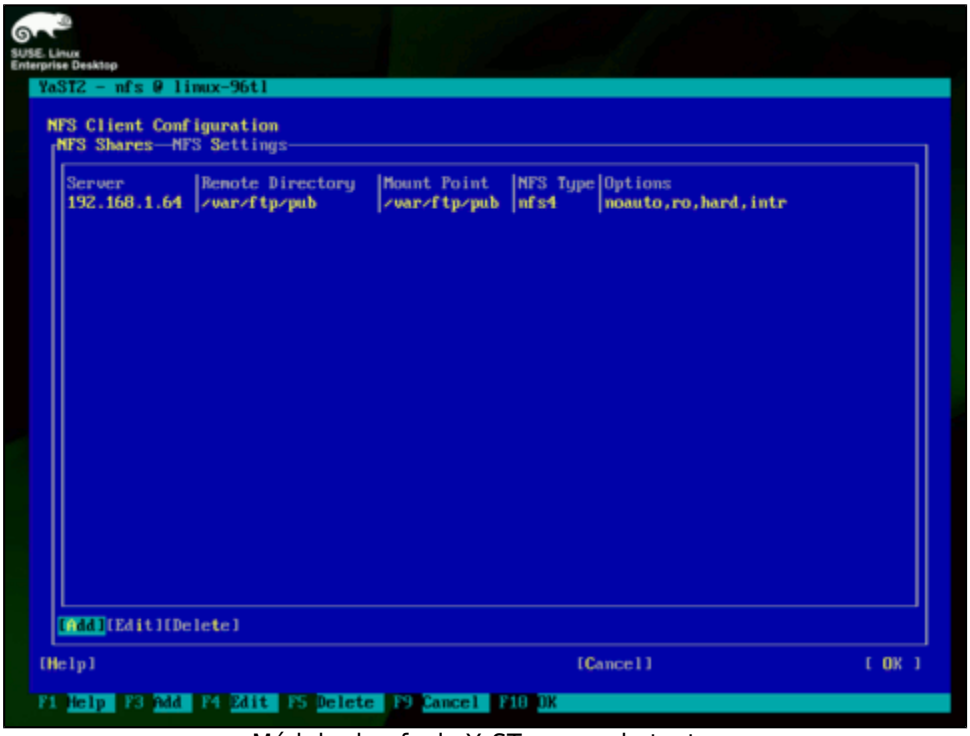
```
man 5 nfs
```

53.7.4. Modulo nfs de YaST en openSUSE y SUSE Linux Enterprise.

Para configurar los sistemas de archivos remotos para ser montados en el sistema de archivos local, el método preferido es utilizar el módulo **nfs** de YaST. Ejecute lo siguiente:

```
yast nfs
```

Defina los servidores, directorios remotos, puntos de montaje y opciones a utilizar y aplique los cambios.



Módulo de nfs de YaST, en modo texto.

53.8. Ejercicios.

53.8.1. Compartir un volumen NFS para acceso público.

Si acaso fuese inexistente, genere el directorio local **/var/ftp/pub**:

```
test -d /var/ftp/pub || mkdir -p /var/ftp/pub
```

Copie cualquier contenido de acceso público dentro de este directorio.

Para compartir el directorio local **/var/ftp/pub** en modo de **sólo lectura** (**ro**), edite el archivo **/etc/exports**:

```
vi /etc/exports
```

Asumiendo que se trata del directorio público de el servidor FTP del sistema, que éste se compartirá en modo de **sólo lectura** (opción **ro**) convirtiendo todos los UID y GID de los clientes al usuario anónimo de NFS (opción **all_squash**), a toda la red de área local y que ésta corresponde a **192.168.70.0/25**, añada el siguiente contenido:

```
/var/ftp/pub    192.168.70.0/25(ro,all_squash)
```

Si utiliza CentOS, Fedora o Red Hat Enterprise Linux, ejecute lo siguiente para aplicar los cambios:

```
service nfs restart
```

Si utiliza openSUSE o SUSE Linux Enterprise Server, ejecute lo siguiente para aplicar los cambios:

```
rcnfsserver restart
```

53.8.1.1. Acceso desde los clientes NFS.

Como root, desde el anfitrión cliente, ejecute el mandato **showmount** con la opción **-e** para consultar los volúmenes exportados por el servidor NFS:

```
showmount -e 192.168.70.2
```

La salida debe ser similar a la siguiente:

```
Export list for 192.168.70.2:
/var/ftp/pub          192.168.70.0/25
```

Si acaso fuese inexistente, genere el directorio local **/var/ftp/pub**:

```
test -d /var/ftp/pub || mkdir -p /var/ftp/pub
```

Monte el directorio remoto **192.168.70.2:/var/ftp/pub** en el directorio local **/var/ftp/pub:**

```
mount -o hard,intr,ro 192.168.70.2:/var/ftp/pub /var/ftp/pub
```

Verifique con el mandato **df** que se ha montado con éxito el directorio remoto.

```
df -h
```

Para configurar permanentemente el directorio remoto, edite el archivo **/etc/fstab**:

```
vi /etc/fstab
```

Añada el siguiente contenido:

```
192.168.70.2:/var/ftp/pub  /var/ftp/pub  nfs4  hard,intr,ro  0 0
```

Reinicie el sistema y verifique que el directorio remoto montó exitosamente.

53.9. Bibliografía.

- es.wikipedia.org/wiki/Network_File_System

54. Configuración básica de Samba.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales (incluyendo su publicación, a través de cualquier medio, por entidades con fines de lucro). c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en castellano. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

54.1. Introducción.

54.1.1. Acerca del protocolo SMB.

SMB (acrónimo de ***S****erver* ***M****essage* ***B****lock*) es un protocolo, del **Nivel de Presentación** del modelo OSI de TCP/IP, creado en 1985 por IBM. Algunas veces es referido también como **CIFS** (Acrónimo de ***C****ommon* ***I****nternet* ***F****ile* ***S****ystem*, http://samba.org/cifs/) tras ser renombrado por Microsoft en 1998. Entre otras cosas, Microsoft añadió al protocolo soporte para enlaces simbólicos y duros así como también soporte para archivos de gran tamaño. *Por mera coincidencia*, ésto ocurrió por la misma época en que Sun Microsystems hizo el lanzamiento de WebNFS (una versión extendida de **NFS**, http://www.sun.com/software/webnfs/overview.xml).

SMB fue originalmente diseñado para trabajar a través del protocolo NetBIOS, el cual a su vez trabaja sobre **NetBEUI** (acrónimo de ***N****etBIOS* ***E****xtended* ***U****ser* ***I****nterface*, que se traduce como Interfaz de Usuario Extendida de NetBIOS), **IPX/SPX** (acrónimo de ***I****nternet* ***P****acket E****x****change/****S****equenced* ***P****acket E****x****change*, que se traduce como **Intercambio de paquetes inter-red/Intercambio de paquetes secuenciales**) o **NBT**, aunque también puede trabajar directamente sobre **TCP/IP**.

54.1.2. Acerca de Samba.

SAMBA es un conjunto de programas originalmente creados por Andrew Tridgell y actualmente mantenidos por *The SAMBA Team*, bajo la Licencia Publica General GNU y que implementan en sistemas basados sobre UNIX™ el protocolo **SMB**. Sirve como reemplazo total para Windows™ NT, Warp™, NFS™ o servidores Netware™.

54.2. Equipamiento lógico necesario.

Necesitará tener instalados los siguientes paquetes:

- samba: Servidor SMB.
- samba-client: Diversos clientes para el protocolo SMB.
- samba-common: Archivos necesarios para cliente y servidor.

Instalación a través de yum.

Si utiliza **CentOS**, **Fedora™** o **Red Hat™ Enterprise Linux**, sólo ejecute:

```
yum -y install samba samba-client samba-common
```

En el caso de **CentOS 6** y **Red Hat™ Enterprise Linux 6**, se instalará **Samba 3.6.9**.

En el caso de **CentOS 5** y **Red Hat™ Enterprise Linux 5**, se instalará **Samba 3.0.33**, sin embargo hay opción a utilizar en su lugar **Samba 3.5.4** instalando los paquetes **samba3x**, **samba3x-client** y **samba3x-common**.

```
yum remove samba samba-client samba-common
yum -y install samba3x samba-client3x samba-common3x
```

54.3. Modificaciones necesarias en el muro cortafuegos.

Es necesario abrir los puertos 135 al 139 por TCP y UDP y el puerto 445 por TCP.

54.3.1. Servicio iptables.

Puede utilizar directamente el mandato **iptables** ejecutando lo siguiente:

```
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 135:139 -j ACCEPT
iptables -A INPUT -m state --state NEW -m udp -p udp --dport 135:139 -j ACCEPT
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 445 -j ACCEPT

service iptables save
```

O bien edite el archivo **/etc/sysconfig/iptables**:

```
vim /etc/sysconfig/iptables
```

Y añada el siguiente contenido:

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 135:139 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 135:139 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 445 -j ACCEPT
```

Para aplicar los cambios, reinicie el servicio **iptables**:

```
service iptables restart
```

54.3.2. Shorewall.

Edite el archivo **/etc/shorewall/rules**:

```
vim /etc/shorewall/rules
```

Para permitir el acceso desde cualquier zona del muro cortafuegos o si sólo se tiene una zona en el muro cortafuegos, las reglas corresponderían a algo similar a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  all     fw      tcp     135:139,445
ACCEPT  all     fw      udp     135:139
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Sí se tienen varias zonas en el muro cortafuegos y sólo se desea permitir el acceso desde la zona correspondiente a red local, ejecute.

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  loc     fw      tcp     135:139,445
ACCEPT  loc     fw      udp     135:139
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Al terminar de configurar las reglas para **Shorewall**, reinicie el muro cortafuegos, ejecutando el siguiente mandato:

```
service shorewall restart
```

54.4. SELinux y el servicio smb.

A fin de que SELinux permita al servicio **smb** la escritura como usuario anónimo, ejecute:

```
setsebool -P allow_smbd_anon_write 1
```

A fin de que SELinux permita al servicio **smb** funcionar como Controlador Primario de Dominio (**PDC**, **P**rimary **D**omain **C**ontroler), ejecute:

```
setsebool -P samba_domain_controller 1
```

A fin de que SELinux permita al servicio **smb** compartir los directorios de inicio de los usuarios locales del sistema, ejecute:

```
setsebool -P samba_enable_home_dirs 1
```

A fin de que SELinux desactive la protección para los directorios de inicio de los usuarios a través del servicio **smb**, ejecute:

```
setsebool -P use_samba_home_dirs 1
```

A fin de que SELinux permita al servicio **smb** crear nuevos directorios de inicio para los usuarios a través de PAM (operación común en Controladores Primarios de Dominio), ejecute:

```
setsebool -P samba_create_home_dirs 1
```

A fin de que SELinux permita al servicio **smb** funcionar como un organizador de mapa de puertos (*portmappper*), ejecute:

```
setsebool -P samba_portmapper 1
```

A fin de que SELinux permita al servicio **smb** ejecutar guiones dentro del directorio **/var/lib/samba/scripts** en sin confinamiento, ejecute:

```
setsebool -P samba_run_unconfined 1
```

A fin de que SELinux permita al servicio **smb** compartir todos los recursos en modo de sólo lectura, ejecute:

```
setsebool -P samba_export_all_ro 1
```

A fin de que SELinux permita al servicio **smb** compartir todos los recursos en modo de lectura y escritura, ejecute:

```
setsebool -P samba_export_all_rw 1
```

Para definir que un directorio será compartido a través del servicio **smb**, como por ejemplo **/var/samba/publico** y que se debe considerar como contenido tipo Samba, ejecute:

```
chcon -t samba_share_t /var/samba/publico
```

Cada nuevo directorio que vaya a ser compartido a través de Samba, debe ser configurado como acaba de describirse antes de ser configurado en el archivo **/etc/samba/smb.conf**.

54.5. Iniciar el servicio y añadirlo al arranque del sistema.

Para iniciar los servicios **nmb** y **smb** por primera vez, ejecute:

```
service nmb start
service smb start
```

Si realiza algún cambio en la configuración de la opción **netbios name**, es necesario reiniciar el servicio **nmb**, el cual es el encargado de proveer el servidor de nombres para los clientes a través de NetBIOS sobre IP.

```
service nmb restart
```

Si va a aplicar algún cambio en cualquier otra opción de la configuración, como son los recursos compartidos, sólo es necesario reiniciar el servicio **smb**:

```
service smb restart
```

Para que los servicios **nmb** y **smb** inicien automáticamente junto con el sistema, sólo utilice los dos siguientes mandato:

```
chkconfig nmb on
chkconfig smb on
```

54.6. Procedimientos.

54.6.1. Alta de cuentas de usuario.

Asigne una contraseña al usuario **root**. Ésta puede ser distinta a la utilizada en el sistema.

```
smbpasswd -a root
```

Es importante sincronizar las cuentas entre el servidor **Samba** y las estaciones Windows™. Es decir, si en una máquina con Windows™ ingresamos como el usuario *fulano* con contraseña *123qwe*, en el servidor **Samba** deberá existir también dicha cuenta con ese mismo nombre y la misma contraseña. Como la mayoría de las cuentas de usuario que se utilizarán para acceder hacia **Samba** no requieren acceso al intérprete de mandatos del sistema, no es necesario asignar contraseña con el mandato **passwd** y se deberá definir **/sbin/nologin** o bien **/bin/false** como intérprete de mandatos para la cuenta de usuario involucrada.

```
useradd -s /sbin/nologin usuario
smbpasswd -a usuario
```

Es opcional asignar contraseña con el mandato **passwd**. Cualquier cuenta de usuario a la cual se haya omitido asignar contraseña a través del mandato **passwd**, estará como **cuenta inactiva** para el resto de los servicios.

Si se necesita que las cuentas se puedan utilizar para acceder hacia otros servicios como serían Telnet, SSH, etc, es decir, que se permita acceso al intérprete de mandatos, será necesario especificar **/bin/bash** como intérprete de mandatos y además se deberá asignar una contraseña en el sistema con el mandato **passwd**:

```
useradd -s /bin/bash usuario
passwd usuario
smbpasswd -a usuario
```

54.6.2. El archivo lmhosts

Es necesario empezar resolviendo de manera local los nombres **NetBIOS**, asociándolos con las direcciones IP correspondientes, en el archivo **/etc/samba/lmhosts** (lmhosts es acrónimo de **L**AN **M**anager **h**osts). Edite el archivo **/etc/samba/lmhosts** con cualquier editor de texto simple.

```
vim /etc/samba/lmhosts
```

El nombre *NetBIOS* debe tener un **máximo de doce caracteres alfanuméricos**. Normalmente se utiliza el nombre corto del servidor, bien o el nombre corto que se asigno como alias a la interfaz de red. Si se edita el archivo **/etc/samba/lmhosts**, se encontrará un contenido similar al siguiente:

```
127.0.0.1       localhost
```

Se pueden añadir los nombres y direcciones IP de cada uno de los anfitriones de la red local. Como mínimo debe definirse el nombre del anfitrión del servidor **Samba**, junto con su correspondiente dirección IP:

```
127.0.0.1       localhost
192.168.70.1     servidor
```

De manera opcional, también puede añadir el resto de los anfitriones de la red local. La separación de campos se hace con un tabulador. Ejemplo:

```
127.0.0.1        localhost
192.168.70.1     servidor
192.168.70.2     joel
192.168.70.3     blanca
192.168.70.4     alejandro
192.168.70.5     sergio
192.168.70.6     isaac
192.168.70.7     finanzas
192.168.70.8     direccion
```

54.6.3. Opciones principales del archivo smb.conf.

Edite el archivo **/etc/samba/smb.conf** con cualquier editor de texto simple.

```
vim /etc/samba/smb.conf
```

Dentro de este archivo, encontrará información que será de utilidad y que está comentada con almohadillas (símbolo **#**) y varios ejemplos comentados con punto y coma (símbolo **;**), siendo estos últimos los que se pueden tomar como referencia para configurar.

54.6.3.1. Opción workgroup.

Se utiliza para establecer el grupo de trabajo:

```
workgroup = MIGRUPO
```

54.6.3.2. Opción netbios name.

Permite establecer arbitrariamente un nombre de anfitrión distinto al detectado automáticamente. Este nombre de anfitrión deberá corresponder con el establecido en el archivo **/etc/samba/lmhosts**:

```
netbios name = servidor
```

54.6.3.3. Opción server string.

Es de carácter informativo para los usuarios de la red de área local. Permite definir una descripción breve acerca del servidor.

```
server string = Servidor Samba %v en %L
```

54.6.3.4. Opción hosts allow.

Permite establecer seguridad adicional estableciendo la lista de control de acceso de anfitriones. En ésta se pueden definir direcciones IP individuales o redes que tendrán permiso de acceso hacia el servidor. Si, por mencionar un ejemplo, la red consiste en las anfitriones con dirección IP que van desde 192.168.70.1 hasta 192.168.70.254, el rango de direcciones IP que se definirá en **hosts allow** será «**192.168.70.**», de modo tal que sólo se permitirá el acceso dichas máquinas. En el siguiente ejemplo se definen las redes 192.168.70.0/24 y 192.168.37.0/24, especificando los tres primeros octetos de la dirección IP de red, así como cualquier dirección IP de la red 127.0.0.0/8 (retorno del sistema o *loopback*), siendo necesario definir sólo el primer octeto de dicho segmento:

```
hosts allow = 127., 192.168.70., 192.168.37.
```

54.6.3.5. Opción name resolve order.

De modo predeterminado está ausente de la configuración. Puede añadirla después de la opción mencionada arriba. Define el orden a través del cual se tratará de resolver los nombres NETBIOS. Si utiliza el siguiente ejemplo, se establece que primero se intentará resolver los nombres NETBIOS con la información del archivo **/etc/samba/lmhosts**, luego el archivo **/etc/hosts**, luego a través de consultas en el servidor WINS y, si todo lo anterior falla, a través de la dirección IP de difusión de la red local.

```
name resolve order = lmhosts hosts wins bcast
```

Si se va a utilizar un servidor WINS **en otro servidor** o se está configurando el sistema sólo como cliente SMB, se pueden agilizar las comunicaciones con el resto de los equipos de la red local estableciendo **wins** como la primera opción para resolución de nombres NETBIOS:

```
name resolve order = wins lmhosts hosts bcast
```

Nota.

Nautilus, el gestor de archivos predeterminado del escritorio de GNOME, requiere que esté presente esta última configuración en el archivo **/etc/samba/smb.conf** del anfitrión desde el cual se ejecute y que además se especifique **wins** en el orden de resolución de nombres del archivo **/etc/nsswitch.conf** del anfitrión desde el cual se ejecute. De otro modo Nautilus mostrará invariablemente un error cada vez que se intente conectar a cualquier servidor de red utilizando un nombre NETBIOS.

Guarde el archivo /etc/samba/smb.conf, regrese al intérprete de mandatos y edite el archivo **/etc/nsswitch.conf**:

```
vim /etc/nsswitch.conf
```

En CentOS 6 y Red Hat™ Enterprise Linux 6, alrededor de la línea 38, localice lo siguiente:

```
hosts:      files dns
```

Añada **wins** después de **dns**:

```
hosts:      files dns wins
```

En versiones recientes de Fedora™ openSUSE™ o Ubuntu™, encontrará lo siguiente alrededor de la línea 63:

```
files mdns4_minimal [NOTFOUND=return] dns
```

Añada **wins** después de **dns**:

```
files mdns4_minimal [NOTFOUND=return] dns wins
```

54.6.3.6. Opción interfaces.

Permite establecer desde que interfaces de red del sistema se escucharán peticiones. **Samba** rechazará todas las conexiones provenientes desde cualquier otra interfaz o dirección IP, sin definir. Ésto es útil cuando **Samba** se ejecuta en un servidor que sirve además de puerta de enlace para la red local, impidiendo se establezcan conexiones hacia este servicio desde Internet o bien fuera del bloque o segmento, de direcciones de la red local.

Los valores aceptados para esta opción consisten una lista separada por comas o espacios, con los nombres de las interfaces (lo, eth0, eth1, etc.) y direcciones IP utilizada en una interfaz en particular, con la máscara de sub-red en formato **CIDR** (**C**lassless **I**nter-**D**omain **R**outing), es decir, expresada en bits. Ejemplo:

```
interfaces = lo, eth1, 192.168.70.254/25
```

54.6.4. Opción remote announce.

La opción **remote announce** se encarga de que el servidor Samba se anuncie a si mismo de forma periódica hacia uno o más grupos de trabajo específicos. Se utiliza cuando se necesita que el servidor **Samba** aparezca en otros grupos de trabajo existentes en la red de área local. El grupo de trabajo de destino puede estar en donde sea, mientras exista una ruta y sea posible la difusión exitosa de paquetes.

Los valores que pueden ser utilizados son direcciones IP de difusión (**broadcast**) de la red utilizada (es decir la última dirección IP del segmento de red) y/o nombres de grupos de trabajo. En el siguiente ejemplo se define que el servidor **Samba** se anuncie a través de las direcciones IP de difusión **192.168.70.127** (que corresponde a la dirección IP de difusión de la red **192.168.70.0/25**) y **192.168.2.255** (que corresponde a la dirección IP de difusión de la red **192.168.2.0/24**), hacia los grupos de trabajo **DOMINIO1** y **DOMINIO2** que corresponden a estas redes.

```
remote announce = 192.168.70.127/DOMINIO1, 192.168.2.255/DOMINIO2
```

Para aplicar los cambios, reinicie los servicios **smb** y **nmb**:

```
service smb restart
service nmb restart
```

54.6.5. Impresoras en Samba.

Las impresoras se comparten de modo predeterminado, así que sólo hay que realizar algunos ajustes. Si se desea que se pueda acceder hacia la impresora como usuario invitado sin contraseña, basta con añadir **public = Yes** (que es lo mismo que **guest ok = Yes**) en la sección de impresoras. Edite el archivo /etc/samba/smb.conf:

```
vim /etc/samba/smb.conf
```

Localice la sección de impresoras y añada public = Yes a la configuración:

```
[printers]
        comment = El comentario que guste.
        path = /var/spool/samba
        printable = Yes
        browseable = No
        writable = no
        printable = yes
        public = Yes
```

Para aplicar los cambios, reinicie el servicio **smb**:

```
service smb restart
```

Para la administración de las colas de impresión, anteriormente se hacía utilizando la opción **printer admin**, definiendo una lista de usuarios o grupos. Actualmente se hace de manera similar a cómo se hace en en Windows, utilizando políticas, ejecute:

```
net -S servidor -U root rpc rights grant fulano SePrintOperatorPrivilege
```

54.6.6. Compartiendo directorios a través de Samba.

Para los directorios o volúmenes que se irán a compartir, en el mismo archivo de configuración encontrará distintos ejemplos para distintas situaciones particulares. En general, puede utilizar el siguiente ejemplo que funcionará para la mayoría:

```
[lo_que_sea]
        comment = Comentario que se le ocurra
        path = /cualquier/ruta/que/desee/compartir
```

Procure que los nombres de los recursos a compartir tengan un máximo de 12 caracteres, utilizando sólo caracteres alfanuméricos de la tabla de caracteres ASCII.

El volumen puede utilizar cualquiera de las siguientes opciones:

Opción	**Descripción**
`guest ok`	Define si se permitirá el acceso como usuario invitado. El valor puede ser `Yes` o `No`.
`public`	Es un **equivalente** de la aopción **guest ok**, es decir define si se permitirá el acceso como usuario invitado. El valor puede ser `Yes` o `No`.
`browseable`	Define si se permitirá mostrar este recurso en las listas de recursos compartidos. El valor puede ser `Yes` o `No`.
`writable`	Define si se permitirá la escritura. Es la opción contraria de `read only`. El valor puede ser `Yes` o `No`. Ejemplos: «`writable = Yes`» **es lo mismo que** «`read only = No`». Obviamente «`writable = No`» **es lo mismo que** «`read only = Yes`»
`valid users`	Define los usuarios o grupos, que podrán acceder al recurso compartido. Los valores pueden ser nombres de usuarios separados por comas o bien nombres de grupo antecedidos por una @. Ejemplo: `fulano, mengano, @administradores`
`write list`	Define los usuarios o grupos, que podrán acceder con permiso de escritura. Los valores pueden ser nombres de usuarios separados por comas o bien nombres de grupo antecedidos por una @. Ejemplo: `fulano, mengano, @administradores`
`admin users`	Define los usuarios o grupos, que podrán acceder con permisos administrativos para el recurso. Es decir, podrán acceder hacia el recurso realizando todas las operaciones como super-usuarios. Los valores pueden ser nombres de usuarios separados por comas o bien nombres de grupo antecedidos por una @. Ejemplo: `fulano, mengano, @administradores`
`directory mask`	Es lo mismo que `directory mode`. Define qué permiso en el sistema tendrán los subdirectorios creados dentro del recurso. Ejemplos: `1777`
`create mask`	Define que permiso en el sistema tendrán los nuevos archivos creados dentro del recurso. Ejemplo: `0644`

En el siguiente ejemplo se compartirá a través de Samba el recurso denominado **ejemplo**, el cual está localizado en el directorio **/var/samba/ejemplo** del disco duro. Se permitirá el acceso a cualquiera pero será un recurso de sólo lectura salvo para los usuarios administrador y fulano. Todo directorio nuevo que sea creado en su interior tendrá permiso **755** (**drwxr-xr-x**) y todo archivo que sea puesto en su interior tendrá permisos **644** (**-rw-r--r--**).

Genere el nuevo directorio **/var/samba/ejemplo** ejecutando lo siguiente:

```
mkdir -p /var/samba/ejemplo
```

Cambie el contexto de SELinux, a fin de que este directorio sea considerado como contenido Samba.

```
chcon -t samba_share_t /var/samba/ejemplo
```

Cambie asigne permisos de lectura, escritura y ejecución a los usuarios fulano y zutano:.

```
setfacl -m u:fulano:7,u:zutano:7 /var/samba/ejemplo
```

Edite el archivo **/etc/samba/smb.conf**:

```
vim /etc/samba/smb.conf
```

Al final del archivo añada el siguiente contenido:

```
[ejemplo]
        comment = Recurso de ejemplo
        path = /var/samba/ejemplo
        guest ok = Yes
        read only = Yes
        write list = fulano, zutano
        directory mask = 0755
        create mask = 0644
```

Para aplicar los cambios, reinicie el servicio **smb**:

```
service smb restart
```

54.6.6.1. Ocultando archivos que inician con punto.

Es poco conveniente que los usuarios puedan acceder, notando la presencia de archivos ocultos (archivos de configuración, por lo general), es decir archivos cuyo nombre comienza con un punto, como es el caso del directorio de inicio del usuario en el servidor **Samba** (.bashrc, .bash_profile, .bash_history, etc.). Puede utilizarse la opción **hide dot files**, con el valor **Yes**, para mantenerlos ocultos.

```
hide dot files = Yes
```

Esta opción es útil para complementar la configuración de los directorios personales de los usuarios.

Edite el archivo **/etc/samba/smb.conf**:

```
vim /etc/samba/smb.conf
```

Localice la configuración correspondiente a los directorios de inicio de los usuarios y añada la opción **hide dot files** con el valor **Yes**, como se muestra a continuación:

```
[homes]
   comment = Home Directories
   browseable = no
   writable = yes
   hide dot files = Yes
```

Para aplicar los cambios, reinicie el servicio **smb**:

```
service smb restart
```

54.7. Comprobaciones.

54.7.1. Modo texto desde GNU/Linux.

54.7.1.1. Montaje de recursos compartidos desde GNU/Linux.

Desde un cliente GNU/Linux, abra una terminal y utilice el mandato **mkdir** para crear un punto de montaje:

```
mkdir /mnt/ejemplo
```

Utilice el mandato **mount**, con la opción **-t** con el valor **cifs**, la opción **-o** para especificar con **username** el nombre de usuario a utilizar, la ruta del recurso compartido en el servidor Samba y el punto de montaje a utilizar:

```
mount -t cifs -o username=fulano //servidor/ejemplo /mnt/ejemplo
```

Lo anterior solicitará se ingrese la contraseña del usuario utilizado en el servidor Samba especificado.

Para hacer permanente lo anterior, utilice un editor de texto para crear el archivo **/etc/credentials**:

```
vim /etc/credentials
```

Añada el siguiente contenido, especificando el nombre de usuario y contraseña que serán utilizados específicamente con el recurso compartido involucrado:

```
username=fulano
password=contraseña
```

Cambie los permisos de acceso del archivo, de modo que sólo el usuario **root** pueda ver y modificar el contenido de éste:

```
chmod 600 /etc/credentials
```

Edite el archivo **/etc/fstab**:

```
vim /etc/fstab
```

Añada el siguiente contenido, especificando con las opciones **uid** y **gid** los números de **UID** y **GID** del usuario y grupo del anfitrión local que utilizarán el recurso. De modo predeterminado, este recurso será montado automáticamente con el siguiente reinicio de sistema.

```
//servidor/ejemplo   /mnt/ejemplo   cifs   credentials=/etc/credentials,uid=1005,gid=1005   0 0
```

Utilice las opciones **noauto** y **user** si se prefiere que el recurso sea montado manualmente por un usuario del anfitrión local:

```
//servidor/ejemplo   /mnt/ejemplo   cifs   credentials=/etc/credentials,uid=1005,gid=1005,noauto,user
 0 0
```

54.7.1.2. Herramienta smbclient desde GNU/Linux.

Indudablemente el método más práctico y también el más sencillo para utilizar y hacer pruebas de diagnóstico, es el mandato *smbclient*. Éste permite acceder hacía cualquier servidor Samba o Windows™, de modo similar a como se hace con el mandato **ftp** en el intérprete de mandatos.

Para acceder al cualquier recurso de alguna máquina Windows™ o servidor Samba, determine primero que volúmenes o recursos compartidos posee ésta. Utilice el mandato *smbclient* del siguiente modo:

```
smbclient -U usuario -L servidor
```

Lo anterior devolverá una salida similar la siguiente:

```
Domain=[MI-DOMINIO] OS=[Unix] Server=[Samba 3.6.9-151.el6]

         Sharename       Type      Comment
         ---------       ----      -------
         homes           Disk      Home Directories
         netlogon        Disk      Network Logon Service
         ejemplo         Disk      ejemplo
         IPC$            IPC       IPC Service (Servidor Samba 3.5.4-68.el6_0.2 en mi-servidor)
         ADMIN$          IPC       IPC Service (Servidor Samba 3.5.4-68.el6_0.2 en mi-servidor)
         epl5900         Printer   Created by system-config-printer 1.2.x
         hp2550bw        Printer   Created by system-config-printer 1.2.x
Anonymous login successful
Domain=[MI-DOMINIO] OS=[Unix] Server=[Samba 3.6.9-151.el6]

         Server               Comment
         ---------            -------
         mi-servidor          Servidor Samba 3.6.9-151.el6 en mi-servidor

         Workgroup            Master
         ---------            -------
         MI-DOMINIO           MI-SERVIDOR
```

La siguiente corresponde a la sintaxis básica para poder navegar los recursos compartidos por la máquina Windows™ o el servidor SAMBA:

```
smbclient //alguna_maquina/recurso -U usuario
```

Ejemplo:

```
smbclient //SERVIDOR/EJEMPLO -U fulano
```

Después de ejecutar lo anterior, el sistema solicitará se proporcione la contraseña del usuario *fulano* en el equipo denominado *LINUX*.

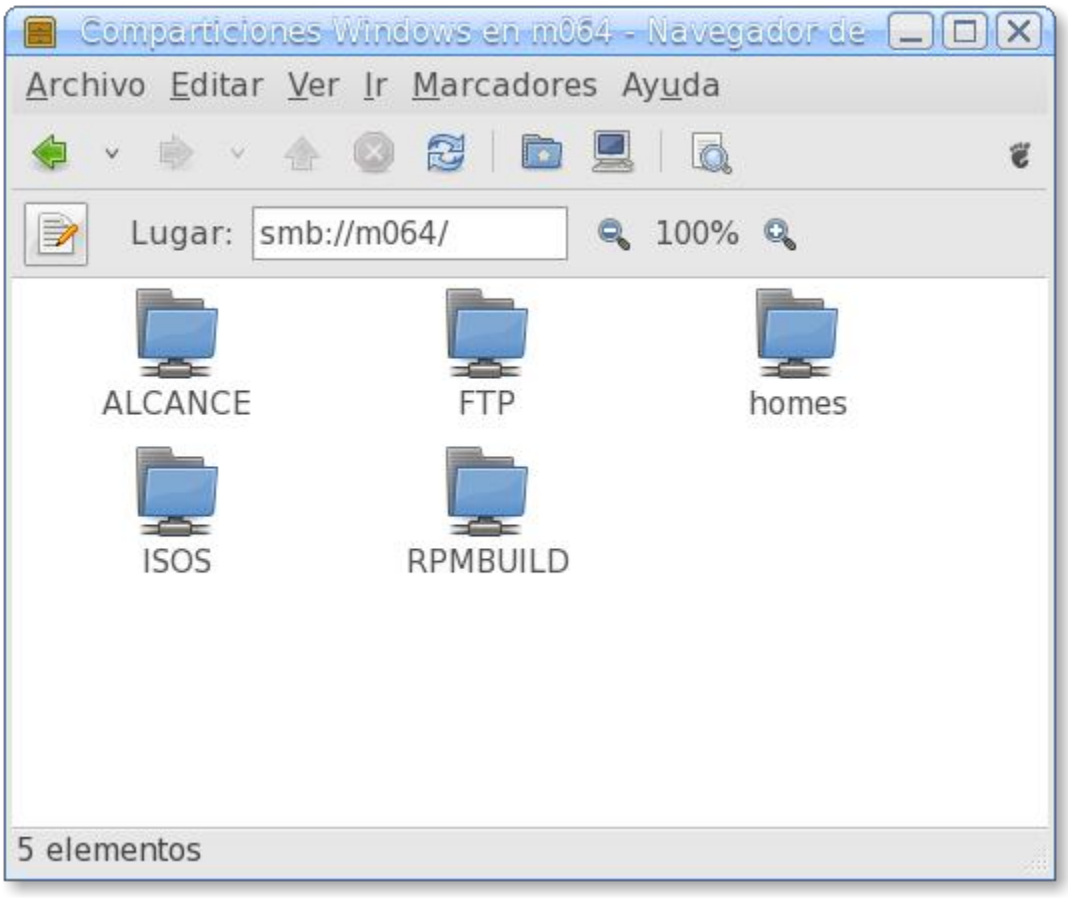
```
smbclient  //SERVIDOR/EJEMPLO -U fulano
added interface ip=192.168.70.126 bcast=192.168.70.127 nmask=255.255.255.128
Password:
Domain=[fulano] OS=[Unix] Server=[Samba 3.6.9-151.el6]
smb: >
```

Pueden utilizarse casi los mismos mandatos que en el intérprete de *ftp*, como serían get, mget, put, del, etc.

54.7.2. Modo gráfico

54.7.2.1. Desde el escritorio de GNOME.

Si utiliza GNOME 2.x o superior, éste incluye un módulo de cliente SMB para Nautilus (**gnome-vfs-smb**, en **CentOS 5** o **gvfs-smb**, en **CentOS 6**), el cual permite acceder hacia los recursos compartidos a través de servidores Samba. Sólo hay que hacer clic en **Servidores de red** (menú de GNOME o bien el mismo Nautilus). Para que funcione correctamente, se requiere que exista un servidor WINS en la red local, se tenga establecida la opción **name resolve order** en el archivo **/etc/samba/smb.conf** y que la opción **hosts** del archivo **/etc/nsswitch.conf** incluya **wins**.



54.7.2.2. Desde Windows.

Desde Windows deberá ser posible acceder sin problemas hacia cualquier servidor **Samba**, como si fuese hacia cualquier otro sistema con Windows.

55. Cómo configurar Samba denegando acceso a ciertos archivos.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales (incluyendo su publicación, a través de cualquier medio, por entidades con fines de lucro). c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en castellano. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

55.1. Introducción.

En algunos casos puede ser necesario denegar el acceso a ciertas extensiones de archivos, como archivos de sistema y archivos de multimedios como MP3, MP4, MPEG y DivX.

Este documento considera que usted ya ha leído previamente, a detalle y en su totalidad el manual «Cómo configurar Samba básico». y que ha configurado exitosamente **Samba** como servidor de archivos.

55.2. Procedimientos.

El parámetro **veto files** se utiliza para especificar la lista, separada por diagonales, de aquellas cadenas de texto que denegarán el acceso a los archivos cuyos nombres contengan estas cadenas. En el siguiente ejemplo, se denegará el acceso hacia los archivos cuyos nombres incluyan la palabra *«Security»* y los que tengan extensión o terminen en *«.tmp»*:

```
[homes]
   comment = Home Directories
   browseable = no
   writable = yes
   hide dot files = Yes
   veto files =  /*Security*/*.tmp/
```

En el siguiente ejemplo, se denegará el acceso hacia los archivos que tengan las extensiones o terminen en *«.mp3»*, *«.mp4»*, *«.mpeg»* y *«.avi»* en todos los directorios personales de todos los usuarios del sistema:

```
[homes]
   comment = Home Directories
   browseable = no
   writable = yes
   hide dot files = Yes
   veto files =  /*.mp3/*.mp4/*.mpg/*.avi/*.tmp/
```

55.3. Aplicando los cambios.

Para hacer que los cambios hechos surtan efecto tras modificar la configuración, utilice:

```
service smb restart
```

55.4. Comprobaciones.

Con la finalizad de realizar pruebas, genere con el mandato **echo** del sistema un archivo denominado **prueba.mp3**:

```
echo "archivo MP3 de pruebas" > prueba.mp3
```

Si aún no existiera, genere al usuario **fulano**:

```
useradd fulano
```

Utilice el mandato **smbpasswd** y asigne **123qwe** como clave de acceso al usuario **fulano**:

```
smbpasswd -a fulano
```

Acceda con **smbclient** hacia el servidor **Samba** con el usuario **fulano**:

```
smbclient //127.0.0.1/fulano -Ufulano%123qwe
```

Lo anterior debe devolver una salida similar a la siguiente:

```
Domain=[M064] OS=[Unix] Server=[Samba 3.2.0rc1-14.9.el5.al]
smb: >
```

Utilizando el mandato **put** del **intérprete SMB**, suba el archivo **prueba.txt** al directorio personal de fulano:

```
smb: > put prueba.mp3
```

Lo anterior debe devolver una salida similar a la siguiente indicando el mensaje **NT_STATUS_OBJECT_NAME_NOT_FOUND** como respuesta, lo cual indica que no fue permitido subir el archivo **prueba.mp3**:

```
smb: > put prueba.mp3
NT_STATUS_OBJECT_NAME_NOT_FOUND opening remote file prueba.mp3
smb: >
```

Para salir del **intérprete SMB** utilice el mandato **exit**:

```
smb: > exit
```

56. Cómo configurar Samba con Papelera de Reciclaje.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales (incluyendo su publicación, a través de cualquier medio, por entidades con fines de lucro). c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en castellano. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

56.1. Introducción.

En algunas circunstancias, es necesario añadir una **Papelera de Reciclaje** (**Recycle Bin**) para evitar la eliminación permanente del contenido de un directorio compartido a través de **Samba**. Es particularmente útil para los directorios personales de los usuario.

Este documento considera que usted ya ha leído previamente, a detalle y en su totalidad el manual «Cómo configurar Samba básico». y que ha configurado exitosamente **Samba** como servidor de archivos.

56.2. Procedimientos

La **Papelera de Reciclaje** se activa añadiendo al recurso a compartir los parámetros **vfs objects** y **recycle:repository** del modo ejemplificado a continuación:

```
[homes]
   comment = Home Directories
   browseable = no
   writable = yes
   vfs objects = recycle
   recycle:repository = Recycle Bin
```

Lo anterior creara el objeto **recycle**, que almacenará los contenidos eliminados desde el cliente en un subdirectorio denominado **Recycle Bin**, el cual es creado si éste no existiera. Si el contenido de **Recycle Bin** es eliminado, éste se hará de forma permanente.

En el caso de directorios compartidos que sean accedidos por distintos usuarios, el subdirectorio **Recycle Bin** se crea con permisos de acceso solo para el primer usuario que elimine contenido. Lo correcto es solo utilizarlo en directorios compartidos que solo sean utilizados por un solo usuario. De ser necesario, se puede cambiar el permiso de acceso del subdirectorio **Recycle Bin** con el mandato **chmod** de **0700** a **1777** para permitir a otros usuarios utilizar éste, tomando en cuenta que de esta forma el contenido conservará los privilegios de cada usuario y los contenidos solo podrán ser eliminados permanentemente por sus propietarios correspondientes.

Se pueden añadir más opciones para lograr un comportamiento más similar al de una **Papelera de Reciclaje** normal en **Windows**. El parámetro **recycle:versions** define que si hay dos o más archivos con el mismo nombre y estos son enviados a la **Papelera de Reciclaje**, se mantendrán todos donde los archivo más recientes tendrán un nombre con el esquema **«Copy #x of nombre-archivo»** (es decir, **Copia #x del nombre-archivo**). El parámetro **recycle:keeptree** define que si se elimina un directorio con subdirectorios y contenido, se mantendrá la estructura de éstos.

```
[homes]
   comment = Home Directories
   browseable = no
   writable = yes
   vfs objects = recycle
   recycle:repository = Recycle Bin
   recycle:versions = Yes
   recycle:keeptree = Yes
```

Se puede definir además que se excluyan archivos (**recycle:exclude**) y directorios (**recycle:exclude_dir**) de ser enviado a la **Papelera de Reciclaje** cierto tipo de contenido y sea eliminado de forma permanente de inmediato. Las listas para archivos y directorios son separadas por tuberías (**|**) y aceptan comodines (***** y **?**). En el siguiente ejemplo se excluyen los archivos con extensiones ***.tmp**, ***.temp**, ***.o**, ***.obj**, **~$***, ***.~??**, ***.log**, ***.trace** y ***.TMP** y los directorios **/tmp**, **/temp** y **/cache**.

```
[homes]
   comment = Home Directories
   browseable = no
   writable = yes
   vfs objects = recycle
   recycle:repository = Recycle Bin
   recycle:versions = Yes
   recycle:keeptree = Yes
   recycle:exclude = *.tmp|*.temp|*.o|*.obj|~$*|*.~??|*.log|*.trace|*.TMP
   recycle:excludedir = /tmp|/temp|/cache
```

Si no se quiere que se guarden versiones distintas de archivos con el mismo nombre, para algunas extensiones, es posible hacerlo definiendo el parámetro **recycle:noversions** y una lista de extensiones de archivos separados por tuberías (**|**). En el siguiente ejemplo, se indica que no se guarden diferentes versiones de archivos con el mismo nombre que tengan las extensiones ***.doc**, ***.ppt**, ***.dat** y ***.ini**.

```
[homes]
   comment = Home Directories
   browseable = no
   writable = yes
   vfs objects = recycle
   recycle:repository = Recycle Bin
   recycle:versions = Yes
   recycle:keeptree = Yes
   recycle:exclude = *.tmp|*.temp|*.o|*.obj|~$*|*.~??|*.log|*.trace|*.TMP
   recycle:excludedir = /tmp|/temp|/cache
   recycle:noversions = *.doc|*.ppt|*.dat|*.ini
```

También es posible definir un mínimo y un máximo de tamaño en **bytes** a través de los parámetros **recycle:minsize**, que define un tamaño mínimo y **recycle:maxsize**, que define un tamaño máximo. Cualquier archivo que esté fuera de estos límites establecidos, será eliminado permanentemente de forma inmediata. En el siguiente ejemplo se define que solo podrán ser enviados a la **Papelera de Reciclaje** los archivos que tengan un tamaño mínimo de 10 bytes y un tamaño máximo de 5120 bytes (5 MB)

```
[homes]
   comment = Home Directories
   browseable = no
   writable = yes
   hide dot files = Yes
   vfs objects = recycle
   recycle:repository = Recycle Bin
   recycle:versions = Yes
   recycle:keeptree = Yes
   recycle:exclude = *.tmp|*.temp|*.o|*.obj|~$*|*.~??|*.log|*.trace|*.TMP
   recycle:excludedir = /tmp|/temp|/cache
   recycle:noversions = *.doc|*.ppt|*.dat|*.ini
```

```
   recycle:minsize = 10
   recycle:maxsize = 5120
```

56.3. Aplicando los cambios.

Para hacer que los cambios hechos surtan efecto tras modificar la configuración, utilice:

```
service smb restart
```

56.4. Comprobaciones.

Con la finalizad de realizar pruebas, genere con el mandato **echo** del sistema un archivo denominado **prueba.txt**:

```
echo "archivo de pruebas" > prueba.txt
```

Si aún no existiera, genere al usuario **fulano**:

```
useradd fulano
```

Utilice el mandato **smbpasswd** y asigne **123qwe** como clave de acceso al usuario **fulano**:

```
smbpasswd -a fulano
```

Acceda con **smbclient** hacia el servidor **Samba** con el usuario **fulano**:

```
smbclient //127.0.0.1/fulano -Ufulano%123qwe
```

Lo anterior debe devolver una salida similar a la siguiente:

```
Domain=[M064] OS=[Unix] Server=[Samba 3.2.0rc1-14.9.el5.al]
smb: >
```

Utilizando el mandato **put** del **intérprete SMB**, suba el archivo **prueba.txt** al directorio personal de fulano:

```
smb: > put prueba.txt
```

Lo anterior debe devolver una salida similar a la siguiente:

```
smb: > put prueba.txt
putting file prueba.txt as prueba.txt (0,4 kb/s) (average 0,4 kb/s)
smb: >
```

Visualice el contenido del directorio actual desde el **intérprete SMB** utilizando el mandato **dir**para verificar que se ha subido el archivo **prueba.txt**:

```
smb: > dir
```

Lo anterior debe devolver una salida similar a la siguiente:

```
smb: > dir
  .                                   D        0  Wed Jun 18 20:44:39 2008
  ..                                  D        0  Wed Jun 18 20:04:14 2008
  .bashrc                             H      124  Wed Jun 18 20:04:14 2008
  .bash_profile                       H      176  Wed Jun 18 20:04:14 2008
  .bash_logout                        H       24  Wed Jun 18 20:04:14 2008
  prueba.txt                          A       19  Wed Jun 18 20:44:39 2008

                34173 blocks of size 524288. 12143 blocks available
smb: >
```

Elimine el archivo **prueba.txt** utilizando el mandato del desde el **intérprete SMB**:

```
smb: > del prueba.txt
smb: >
```

Visualice de nuevo el contenido del directorio con el mandato **dir**, lo cual debe devolver una salida similar a la siguiente donde ha desaparecido el archivo **prueba.txt** y ahora aparece el directorio **Recycle Bin**:

```
smb: > dir
  .                                   D        0  Wed Jun 18 20:52:49 2008
  ..                                  D        0  Wed Jun 18 20:04:14 2008
  .bashrc                             H      124  Wed Jun 18 20:04:14 2008
  .bash_profile                       H      176  Wed Jun 18 20:04:14 2008
  .bash_logout                        H       24  Wed Jun 18 20:04:14 2008
  .zshrc                              H      658  Wed Jun 18 20:04:14 2008
  .kde                               DH        0  Wed Jun 18 20:04:14 2008
  .emacs                              H      515  Wed Jun 18 20:04:14 2008
  Recycle Bin                         D        0  Wed Jun 18 20:52:49 2008

                34173 blocks of size 524288. 12143 blocks available
smb: >
```

Acceda al directorio **Recycle Bin** utilizando el mandato **cd**:

```
smb: > smb: > cd "Recycle Bin"
```

Visualice el contenido con el mandato **dir**, lo cual debe devolver una salida similar a la siguiente donde se muestra que el archivo **prueba.txt**, que fue eliminado con el mandato **del**, ahora está dentro del directorio **Recycle Bin**.

```
smb: Recycle Bin> dir
  .                                   D        0  Wed Jun 18 20:52:49 2008
  ..                                  D        0  Wed Jun 18 20:52:49 2008
  prueba.txt                          A       19  Wed Jun 18 20:44:39 2008

                34173 blocks of size 524288. 12141 blocks available
```

Para salir del **intérprete SMB** utilice el mandato **exit.**

57. Cómo configurar Samba como cliente o servidor WINS.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red:*http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales (incluyendo su publicación, a través de cualquier medio, por entidades con fines de lucro). c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en castellano. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

57.1. Introducción.

WINS (**W**indows **I**nternet **N**ame **S**ervice) es un servidor de nombres de para NetBIOS, que se encarga de mantener una tabla con la correspondencia entre direcciones IP y nombres **NetBIOS**, de los equipos que conforman la red local. Esta lista permite localizar rápidamente a otro equipo dentro de la red. Al utilizar un servidor **WINS** se evita el realizar búsquedas innecesarias a través de difusión (**broadcast**) reduciendo sustancialmente el tráfico de red. La resolución de nombres em **Samba**se lleva a cabo realizando consultas en el siguiente orden:

1. Servidor **WINS**
2. Información del archivo **/etc/samba/lmhosts**
3. Información del archivo **/etc/hosts**
4. Difusión (**broadcast**)

Este documento considera que usted ya ha leído previamente, a detalle y en su totalidad, el manual «Cómo configurar Samba básico». y que ha configurado exitosamente **Samba** como servidor de archivos.

57.2. Procedimientos.

Todos los parámetros descritos a continuación, se definen en la sección **[global]** del archivo **/etc/samba/smb.conf**.

```
vim /etc/samba/smb.conf
```

57.2.1. Parámetros wins server y wins support.

Se puede definir que el servidor **Samba** recién configurado se convierta en un servidor **WINS** o bien utilizar un servidor **WINS** ya existente. **No es posible ser cliente y servidor al mismo tiempo**. Los parámetros **wins server** y **wins support**, que se definen en la sección **[global]** del archivo **/etc/samba/smb.conf**, son mutuamente excluyentes.

Si el sistema va ser utilizado como servidor **WINS**, debe habilitarse el parámetro **wins support** con el valor **yes**:

```
wins support = Yes
```

Si el sistema va a utilizar un servidor **WINS existente**, debe habilitarse el parámetro **wins server** y como valor se especifica la dirección IP que utilice el servidor **WINS**. En el siguiente ejemplo se define al sistema con dirección IP **192.168.1.1** como servidor **WINS**:

```
wins server = 192.168.1.1
```

57.2.2. Parámetro name resolve order

Define en **Samba** el orden de los métodos a través de los cuales se intentará resolver los nombres **NetBIOS**. Pueden definirse hasta hasta cuatro valores: wins, lmhosts, hosts y bcast, como se muestra en el siguiente ejemplo.

```
name resolve order = wins lmhosts hosts bcast
```

57.2.3. Parámetro wins proxy.

Cuando su valor es **yes**, permite a **Samba** como servidor intermediario (**proxy**) para otro servidor **WINS**.

```
wins proxy = yes
```

El valor predeterminado de este parámetro es **no**.

57.2.4. Parámetro dns proxy.

Cuando su valor es **yes**, permite a **Samba** realizar búsquedas en un servidor **DNS** si le es imposible determinar un nombre a través de un servidor **WINS**.

```
dns proxy = yes
```

El valor predeterminado de este parámetro es **no**.

57.2.5. Parámetro max ttl.

El parámetro **max ttl** define el máximo tiempo de vida en segundos para los nombres **NetBIOS** que han sido consultados como cliente **WINS** en un servidor **WINS**. su valor predeterminado es **259200**, que corresponde a tres días. **Por lo general no es necesario modificar este parámetro**. Si las direcciones IP de los equipos que integran la red local cambian demasiado frecuentemente, puede reducirse este tiempo. En el siguiente ejemplo, se definen 48 horas como tiempo máximo de vida para los nombres **NetBIOS**:

```
max ttl = 86400
```

57.2.6. Parámetros max wins ttl y min wins ttl.

Los parámetros **max wins ttl** y **min wins ttl**, corresponden a los tiempos máximo y mínimo, respectivamente, en escala de segundos, que tendrán de vida los nombres **NetBIOS** que han sido asignados por el servidor **Samba**. El valor predeterminado de **max wins ttl**, es **518400**, es decir, 6 días y el valor predeterminado de **min wins ttl**, es **21600**, es decir, 6 horas. **Por lo general no es necesario modificar estos parámetros**. Si las direcciones IP de los equipos que integran la red local cambian muy frecuentemente, pueden modificarse estos tiempos. En el siguiente ejemplo se redundan los valores predeterminados:

```
max wins ttl = 518400
min wins ttl = 21600
```

57.3. Aplicando los cambios.

Para hacer que los cambios hechos surtan efecto tras modificar la configuración, reincie los servicios **smb** y **nmb**:

```
service smb restart
service nmb restart
```

58. Instalación, configuración y optimización de Spamassassin.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

58.1. Introducción.

58.1.1. Acerca de SpamAssassin.

SpamAssassin es una implementación que utiliza un sistema de puntuación, basado sobre algoritmos de tipo genético, para identificar mensajes que pudieran ser sospechosos de ser correo masivo no solicitado, añadiendo cabeceras a los mensajes de modo que pueda ser filtrados por el cliente de correo electrónico o **MUA** (**M**ail **U**ser **A**gent).

URL: http://spamassassin.apache.org/

58.1.2. Acerca de Procmail.

Procmail es un programa que funciona como **MDA** (**M**ail **D**elivery **A**gent o Agente de Entrega de Correo) que se utiliza para gestionar la entrega de correo local en el sistema. Además de lo anterior, permite también realizar filtración automática del correo electrónico, pre-ordenamiento y otras tareas.

Procmail puede ser utilizado indistintamente con Sendmail o bien Postfix.

URL: http://www.procmail.org

58.2. Equipamiento lógico necesario.

58.2.1. Instalación a través de yum.

Si dispone de un servidor con **CentOS 5** o **6** o bien **Red Hat™ Enterprise Linux 5** o **6**, puede utilizar el siguiente mandato:

```
yum -y install spamassassin procmail
```

Si se utiliza Sendmail como servidor de correo electrónico, **procmail** ya debe estar instalado, pues es dependencia del paquete **sendmail**. Si se utiliza Postfix como servidor de correo electrónico, es necesario editar el archivo **/etc/postfix/main.cf** y añadir o descomentar **mailbox_command = /usr/bin/procmail** o bien simplemente ejecutar los siguientes dos mandatos.

```
postconf -e 'mailbox_command = /usr/bin/procmail'
service postfix restart
```

Si se quiere instalar paquetes adicionales para incrementar las capacidades de filtrado de Spamassassin, se pude crear el archivo **/etc/yum.repos.d/AL-Server.repo**. Si dispone de un servidor con **CentOS 5** o **6** o bien **Red Hat™ Enterprise Linux 5** o **6**, puede utilizar el el almacén YUM de **Alcance Libre** para servidores en producción, descargando el archivo **http://www.alcancelibre.org/al/server/AL-Server.repo** dentro del directorio **/etc/yum.repos.d/**:

```
cd /etc/yum.repos.d/
wget -N http://www.alcancelibre.org/al/server/AL-Server.repo
cd
```

Este archivo, que se guarda como **/etc/yum.repos.d/AL-Server.repo**, debe tener el siguiente contenido:

```
[AL-Server]
name=AL Server para Enterprise Linux $releasever
mirrorlist=http://www.alcancelibre.org/al/el$releasever/al-server
gpgcheck=1
gpgkey=http://www.alcancelibre.org/al/AL-RPM-KEY
```

Hecho lo anterior, será posible instalar los paquetes **perl-Mail-SPF**, **perl-Razor-Agent**, **pyzor**, **spamassassin-FuzzyOcr**, **popler-utils** y **re2c**:

```
yum -y install perl-Mail-SPF perl-Razor-Agent pyzor
yum -y install spamassassin-FuzzyOcr poppler-utils re2c
```

58.3. SELinux y el servicio spamasssassin.

58.3.1. Políticas de SElinux.

A fin de que SELinux permita al servicio **spamassassin** conectarse a servicios externos, como **Razor** o **Pyzor**, utilice el siguiente mandado:

```
setsebool -P spamassassin_can_network 1
```

A fin de que SELinux permita a los usuarios del sistema utilizar **spamassassin** desde sus directorios de inicio, utilice el siguiente mandato:

```
setsebool -P spamd_enable_home_dirs 1
```

Nota.

Lo siguiente sólo aplica para **CentOS 5** y **Red Hat™ Enterprise Linux 5**.

Si se desea desactivar toda gestión de SELinux sobre el servicio **spamassassin**, haciendo que todo lo anterior pierda sentido y eliminando la protección que brinda esta implementación, utilice el siguiente mandato:

```
setsebool -P spamd_disable_trans 1
```

Esta política es inexistente en **CentOS 6** y **Red Hat™ Enterprise Linux 6**.

58.3.2. Otros ajustes de SELinux.

A fin de que SELinux permita a **spamassassin** añadir registros a la bitácora del servicio de **Razor**, es necesario generar una nueva política.

Genere un nuevo directorio denominado **/usr/share/selinux/packages/spamd**:

```
mkdir /usr/share/selinux/packages/spamd
```

Cambiarse al directorio **/usr/share/selinux/packages/spamd**:

```
cd /usr/share/selinux/packages/spamd
```

Si se utiliza **CentOS 6** o **Red Hat Enterprise Linux 6**, Descargar el archivo **http://www.alcancelibre.org/linux/secrets/el6/spamd.te**:

```
wget http://www.alcancelibre.org/linux/secrets/el6/spamd.te
```

Editar el archivo recién descargado:

```
vim spamd.te
```

Asegurarse que tenga el siguiente contenido:

```
module spamd 1.0;

require {
        type spamc_t;
        type admin_home_t;
        type sendmail_t;
        type spamd_t;
        type root_t;
        class lnk_file read;
        class fifo_file write;
        class file { ioctl read open getattr append };
}

#============= spamd_t ==============
allow spamd_t root_t:file { ioctl append };
allow spamd_t admin_home_t:file { read ioctl open getattr append };


#============= spamc_t ==============
allow spamc_t sendmail_t:fifo_file write;
allow spamc_t admin_home_t:file { read open };
```

Lo anterior fue obtenido de la salida del mandato **dmesg|grep audit|audit2allow -m spamd>spamd.te** en un sistema donde SELinux impedía a **spamassassin** realizar escritura sobre la bitácora de Razor. En si, define que se permita añadir contenido al archivo **/razor-agent.log**.

Si se utiliza **CentOS 5** o **Red Hat Enterprise Linux 5**, Descargar el archivo **http://www.alcancelibre.org/linux/secrets/el5/spamd.te**:

```
wget http://www.alcancelibre.org/linux/secrets/el5/spamd.te
```

Editar el archivo recién descargado:

```
vim spamd.te
```

Asegurarse que tenga el siguiente contenido:

```
module spamd 1.0;

require {
        type spamc_t;
        type sendmail_t;
        type spamd_t;
        type root_t;
        class lnk_file read;
        class fifo_file write;
        class file { ioctl append };
}

#============= spamd_t ==============
allow spamd_t root_t:file { ioctl append };

#============= spamc_t ==============
allow spamc_t sendmail_t:fifo_file write;
```

A continuación, se genera el archivo de módulo para SELinux (**spamd.mod**) utilizando el mandato **checkmodule** de la siguiente forma:

```
checkmodule -M -m -o spamd.mod spamd.te
```

Luego, se procede a empaquetar el archivo **spamd.mod** como el archivo **spamd.pp**:

```
semodule_package -o spamd.pp -m spamd.mod
```

Finalmente se vincula el archivo **spamd.pp** obtenido con las políticas actuales de SELinux y se cargan éstas en el núcleo en ejecución:

```
semodule -i /usr/share/selinux/packages/spamd/spamd.pp
```

Una vez cargadas las nuevas políticas, se pueden eliminar los archivos **spamd.te** y **spamd.mod**, pues sólo será necesario que exista el archivo binario **spamd.pp**.

58.4. Procedimientos.

58.4.1. Iniciar el servicio y añadirlo a los servicios de arranque del sistema.

```
chkconfig spamassassin on
service spamassassin restart
```

Cabe señalar, que sólo es necesario utilizar el servicio **spamassassin** si el servidor de correo electrónico dispone de una gran cantidad de usuarios o bien tiene una elevada cantidad de tráfico. Si se dispone de pocos usuarios, es posible utilizar el mandato **spamassassin** a través del archivo **/etc/procmailrc** o bien **~/.procmailrc**.

58.4.2. Configuración de Procmail.

Hay tres formas de utilizar Procmail para hacer uso de Spamassassin.

58.4.2.1. Utilizando el mandato spamassassin.

La forma más simple de utilizar Spamassassin es haciendo uso del mandato con el mismo nombre. Funciona bien sólo si se tienen pocos usuarios, pues genera una instancia de éste cada vez que se utiliza o llega un mensaje de correo electrónico al sistema. La siguiente es la configuración recomendada para el archivo **/etc/procmailrc**, sí se desea que aplique a todos los usuarios del sistema o bien el archivo **~/.procmailrc** del directorio de inicio de un usuario en particular, si sólo se desea que sea utilizado por algunos usuarios:

```
:0fw
| /usr/bin/spamassassin
```

Sí se dispone de muchos usuarios, es más conveniente utilizar el mandato **spamc**, mismo que requiere esté funcionado el servicio **spamassassin**. La siguiente es la configuración recomendada para el archivo **/etc/procmailrc**, sí se desea que aplique a todos los usuarios del sistema o bien el archivo **~/.procmailrc** del directorio de inicio de un usuario en particular, si sólo se desea que sea utilizado por algunos usuarios:

```
:0fw
| /usr/bin/spamc
```

Todo lo anterior hace que el correo electrónico sea examinado y marcado como *Spam* si alcanza una cantidad suficiente de puntos. Si se desea realizar un filtrado enviando el correo calificado como *Spam* hacia una capeta de correo (**~/mail/Spam**), se puede utilizar lo siguiente:

```
:0fw
| /usr/bin/spamc

# Los mensajes marcados como spam se almacenan en carpeta de spam
:0:
* ^X-Spam-Status: Yes
$HOME/mail/Spam
```

58.4.3. Configuración del archivo /etc/mail/spamassassin/local.cf.

Edite el archivo **/etc/mail/spamassassin/local.cf**.

```
vim /etc/mail/spamassassin/local.cf
```

Se pueden modificar y añadir parámetros con valores, entre los cuales se pueden configurar los siguientes:

required_hits	Se utiliza para establecer la cantidad de puntos acumulados y asignados por **SpamAssassin**, en un mensaje para considerar el éste como Spam. El valor predeterminado es **5**, acepta decimales y se puede ajustar con un valor inferior o mayor de acuerdo al criterio del administrador. Ejemplo: 4.5
report_safe	Determina si el mensaje, si es calificado como spam, se incluye en un adjunto, con el valor 1 o se deja el mensaje tal y como está, con el valor 0. El valor predeterminado es **0**.
rewrite_header	Define con que cadena de caracteres se añadirá al mensaje para identificarlo como Spam. El valor predeterminado es **[SPAM]** y puede cambiarse por lo que considere apropiado el administrador. Ejemplo: **rewrite_header Subject [Spam?]**
whitelist_from	Se utiliza para definir que jamás se considere como Spam los mensajes de correo electrónico cuyo remitente sea un dominio o cuenta de correo electrónico en particular. Se pueden definir varias líneas. Ejemplo: whitelist_from *@midominio.algo whitelist_from *@alcancelibre.org whitelist_from 201.161.1.226
whitelist_to	Si utiliza una lista de correo electrónico (**majordomo** o **mailman**) y se desea evitar que accidentalmente se considere Spam un mensaje de correo electrónico emitido por una de estas listas, se puede definir que nunca se considere Spam el correo emitido por dicha lista. Ejemplo: whitelist_to mailman-users@algo.algo
blacklist_from	Se puede definir que todo el correo electrónico proveniente de un dominio o cuenta de correo electrónico en particular siempre sea considerado como Spam. Ejemplo: blacklist_from alguien@spammer.com

Hay una herramienta de configuración de SpamAssassin, que permite generar el archivo **/etc/mail/spamassassin/local.cf**, en http://www.yrex.com/spam/spamconfig.php.

De primera instancia, añada al archivo **/etc/mail/spamassassin/local.cf** sus direcciones IP locales con el parámetro **whitelist_from**. Ejemplo:

```
# These values can be overridden by editing ~/.spamassassin/user_prefs.cf
# (see spamassassin(1) for details)

# These should be safe assumptions and allow for simple visual sifting
# without risking lost emails.

required_hits 5
report_safe 0
rewrite_header Subject [SPAM]
whitelist_from 127.0.0.1
whitelist_from 192.168.1.91
whitelist_from 201.161.1.226
```

Sí se utiliza el mandato **spamassassin** en el archivo **/etc/procmailrc** o **~/.procmailrc**, los cambios surten efecto de inmediato. Sí se utiliza el mandato **spamc**, para que surtan efecto los cambios se requiere reiniciar el servicio **spamassassin**:

```
service spamassassin restart
```

58.5. Consejos para sacarle mejor provecho a Spamassassin utilizando sa-learn.

Muchos administradores de servidores utilizan Spamassassin para filtrar los mensajes de correo electrónico que llegan a sus servidores. Si embargo, son muy pocos los que conocen y utilizan la herramienta **sa-learn**, incluida con **Spamassassin**, misma que sirve para entrenar y enseñar a identificar *spam* (o *correo chatarra*) al propio **Spamassassin**.

Esencialmente, el mandato **sa-learn** sirve para *entrenar* al componente clasificador Bayesiano de Spamassassin.

La forma que sugiero consiste en utilizar el cliente de correo electrónico y mover todos los mensajes que se consideren como *spam* a una carpeta destinada para tal finalidad, como por ejemplo **~/mail/Spam** y mover de la carpeta de *spam* todos aquellos mensajes que se consideran como legítimos a cualquier otra carpeta de correo o bien el buzón de entrada.

Acto seguido, se utiliza el mandato **sa-learn**, con las opciones **--spam**, para indicar que se trata de mensajes de spam y la opción **--mbox**, para indica que se trata de un buzón de correo en formato **mbox**, lo cual permitirá examinar todos los mensajes contenidos en éste:

```
sa-learn --spam --mbox ~/mail/Spam
```

Para que los mensajes que se clasificaron incidentalmente como *spam* y que fueron movidos a otra carpeta (como por ejemplo **~/mail/Mensajes**) o bien el buzón de entrada (**/var/spool/mail/usuario**), se utiliza el mandato **sa-learn** con las opciones **--ham**, para indicar que es correo legítimo y que se debe dejar de considerar éste como *spam* y la opción **--mbox**, para indica que se trata de un buzón de correo en formato **mbox**, lo cual permitirá examinar todos los mensajes contenidos en éste:

```
sa-learn --ham --mbox ~/mail/Mensajes
sa-learn --ham --mbox /var/spool/mail/usuario
```

De este modo y considerando que se utiliza el archivo **~/.promailrc**, lo cual sólo aplicaría para el usuario utilizado o bien **/etc/procmailrc**, sí se desea que aplique para todos los usuarios del servidor, contiene algo similar a lo siguiente:

```
MAILDIR=$HOME/mail
LOGFILE=$HOME/mail/log
# send mail through spamassassin
:0fw
| /usr/bin/spamassassin
#Mensjes marcados como spam, ponerlos en carpeta de spam
:0:
* ^X-Spam-Status: Yes
Spam
```

Se conseguirá que la mayoría los mensajes de *spam* similares a los que se movieron a la carpeta **~/mail/Spam**, en adelante serán más fáciles de identificar y filtrar y los mensajes que incidentalmente se clasificaron como *spam*, dejarán de ser clasificados como tales o bien será más difícil que sean clasificados como *spam*.

Todo lo anterior puede ser utilizado como el usuario **root**, lo cual haría que los nuevos filtros creados al *entrenar* a **Spamassassin** apliquen para todos los usuarios o bien como cualquier usuario, lo cual sólo tendrían efecto para éste en particular.

Si alguien tiene interés en aprender más acerca del mandato **sa-learn**, puede hacerlo consultando desde una terminal de texto ejecutando **man sa-learn**.

58.6. Incrementando las capacidades de filtrado.

A fin de enriquecer la capacidad de detección de *spam* de **Spamassassin**, pueden instalarse paquetes opcionales como **perl-Mail-SPF**, **perl-Razor-Agent**. Los tres brindan capacidades adicionales de filtración de *spam*, descritas más adelante y pueden contribuir de manera significativa a reducir la cantidad de *spam* que de otro modo **podría** pasar por alto **Spamassassin**.

Para los todos los procedimientos descritos a continuación, se considera que en el servidor de correo electrónico se utiliza como sistema operativo **CentOS 5** y **6** o bien **Red Hat Enterprise Linux 5** y **6**, se tienen instalados los paquetes **procmail** (requisito del paquete **sendmail** y opcional para el paquete **postfix**) y **spamassassin** y que se tiene configurado al menos lo siguiente en el archivo **/etc/procmailrc**:

```
# send mail through spamassassin
:0fw
| /usr/bin/spamc

# Los mensajes marcados como Spam se almacenan en carpeta ~/mail/Spam
:0:
* ^X-Spam-Status: Yes
$HOME/mail/Spam
```

Primeramente y con la finalidad de actualizar el juego de reglas y filtros de Spamassassin, es conveniente utilizar el mandato **sa-update** de vez en cuando, a lo sumo una o dos veces al mes. Los juegos de reglas y filtros de Spamassassin realmente sufren pocos cambios a lo largo del año y se almacenan en un sub-directorio dentro de **/var/lib/spamassassin/**. Sólo es necesario conservar el sub-directorio con la versión más reciente. El siguiente mandato realizará la consulta y actualización de reglas y filtros de Spamassassin y reiniciará el servicio solamente si se descargó una actualización:

```
sa-update -v && service spamassassin restart
```

La opción -v hace que se muestre una salida que incluye una descripción de los canales actualizados. Si desea una salida limpia, sin mensajes descriptivos, ejecute lo siguiente:

```
sa-update && service spamassassin restart
```

Para instalar el conjunto de paquetes que enriquecerán las capacidades de filtrado de **Spamassassin**, considerando que tiene configurados los almacenes YUM para AL Server de Alcance Libre, ejecute lo siguiente:

```
yum -y install perl-Mail-SPF perl-Razor-Agent pyzor
yum -y install spamassassin-FuzzyOcr poppler-utils
```

Si se utilizan paquetes provenientes de otros almacenes YUM distintos a los de Alcance Libre, el complemento para **Pyzor** incluido dentro de **Spamassassin** requerirá además el paquete **perl-Digest-SHA**:

```
yum -y install perl-Digest-SHA
```

A fin de que **Spamassassin** pueda utilizar los complementos que hacen uso de los complementos que se activan con estos componentes, es necesario reiniciar el servicio **spamassassin**:

```
service spamassassin restart
```

58.6.1. Optimizando Spamassassin.

Si se tiene un servidor de correo electrónico con mucha carga de trabajo, conviene optimizar **spamasassassin** compilando las reglas de éste para convertirlas a formato binario. Para tal fin es necesario que esté instalados los paquetes **re2c** y **gcc**:

```
yum -y install re2c gcc
```

Y enseguida se ejecuta el mandato sa-compile:

```
sa-compile
```

Si la sintaxis del archivo **/etc/mail/spamassassin/local.cf** está correcta, el sistema debe realizar la compilación y almacenar los binarios dentro de **/var/lib/spamassassin/compiled/**. Lo anterior deberá ser repetido cada vez que se realicen modificaciones del archivo **/etc/mail/spamassassin/local.cf** o bien se actualice el conjunto de reglas con el mandato **sa-update**.

58.6.2. ¿Por qué Perl-Mail-SPF, Perl-Razor-Agent, Pyzor, Spamassassin-FuzzyOcr y poppler-utils?

58.6.2.1. Perl-Mail-SPF.

Perl-Mail-SPF Implementa una protección contra la falsificación de direcciones en el envío de correo electrónico conocida como **SPF** (**S**ender **P**olicy **F**ramework o Convenio de Remitentes). Funciona realizando consultas a los servidores DNS en busca del registro TXT para **SPF** que específica los servidores de correo electrónico autorizados para enviar correo electrónico para un dominio en particular.

Para que un dominio en particular o bien el propio dominio, sea excluido de este tipo de filtración, requiere contar con un registro similar al siguiente, lo cual establece que **preferentemente** se descartan como emisores de correo electrónico todos aquellos servidores que carezcan de registro tipo MX o tipo A:

```
dominio.com.    IN      TXT     "v=spf1 a mx ~all"
```

O bien, si se quiere algo más estricto, donde se descartan por completo como emisores de correo electrónico todos aquellos servidores que carezcan de registro tipo MX o tipo A:

```
dominio.com.    IN      TXT     "v=spf1 a mx -all"
```

58.6.2.2. Perl-Razor-Agent.

Perl-Razor-Agent es la implementación Perl de **Razor**, que es una red distribuida y colaborativa dedicada a la detección y filtración de *spam*. Consiste en un catalogo de propagación de *spam* que es actualizado constantemente. Se complementa de manera mutua con **Pyzor**.

58.6.2.3. Pyzor.

Pyzor es similar a **Razor** y funciona de la misma forma como una red distribuida y colaborativa dedicada a la detección y filtración de *spam*. A diferencia de **Perl-Razor-Agent**, está escrito en Python. Se complementa de manera mutua con **Razor**.

58.6.2.4. Spamassassin-FuzzyOcr.

Suele haber casos en los cuales se envían mensajes de *spam* que sólo incluyen una imagen incrustada en el mensaje, con el fin de evadir los filtros de los servidores de correo electrónico. **FuzzyOcr** es un complemento (*plugin*) para **Spamassassin** el cual está enfocado sobre este tipo de *spam*. Utiliza **GOCR** (***G****NU* ***O****ptical* ***C****haracter* ***R****ecognition* o Reconocimiento Óptico de Caracteres de GNU) y otros métodos para analizar el contenido de las imágenes y poder distinguir entre correo ordinario y correo *spam*.

58.6.2.5. Poppler-utils.

Este conjunto de herramientas es utilizado por Spamassassin para gestionar los contenidos de los documentos en formato PDF, particularmente las herramientas como **pdftops**, **pstopnm** y **pdfinfo**. Es altamente recomendado instalarlo.

59. Configuración simple para Antivirus y Antispam.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

59.1. Procedimientos

Si utiliza **ALDOS**, éste ya dispone de la configuración necesaria para instalar todos los paquetes necesarios. Si dispone de un servidor con **CentOS** o **Red Hat™ Enterprise Linux**, puede utilizar el el almacén YUM de **Alcance Libre** para servidores en producción, descargando el archivo **http://www.alcancelibre.org/al/server/AL-Server.repo** dentro del directorio **/etc/yum.repos.d/**:

```
wget -N http://www.alcancelibre.org/al/server/AL-Server.repo \
    -O /etc/yum.repos.d/AL-Server.repo
```

Asumiendo que tiene configurados los almacenes YUM de **Alcance Libre**, instale los paquetes **spamassassin**, **clamav** y **clamav-update**.

```
yum -y install spamassassin clamav clamav-update
```

Active las siguientes políticas de SELinux:

```
setsebool -P clamd_use_jit 1
setsebool -P clamscan_can_scan_system 1
setsebool -P spamassassin_can_network 1
setsebool -P spamd_enable_home_dirs 1
```

Actualice la base de datos del antivirus ClamAV, ejecutando lo siguiente:

```
freshclam
```

Actualice el conjunto de reglas de Spamassassin, ejecutando lo siguiente:

```
sa-update -v
```

Lo anterior deberá indicar qué componentes de **Spamassassin** fueron actualizados.

Nota.

Para optimizar y extender el funcionamiento de **Spamassassin**, estudie el documento titulado «**Cómo instalar y configurar Spamassassin**.»

Utilizando el mandato **touch**, genere el archivo **/etc/procmailrc**:

```
touch /etc/procmailrc
```

Edite el archivo **/etc/procmailrc**:

```
vim /etc/procmailrc
```

Añada el siguiente contenido:

```
SHELL=/bin/sh
# Si desea almacenar toda la información de actividad
# de Procmail en una bitácora, descomente lo siguiente.
#LOGFILE=/var/log/procmail.log

# Configuración basada sobre http://bulma.net/body.phtml?nIdNoticia=1978
# y adecuada y actualizada, por Joel Barrios Dueñas.
AV_REPORT=`/usr/bin/clamscan --stdout --no-summary - | cut -d: -f 2`
VIRUS=`if [ "$AV_REPORT" != " OK" ]; then echo Yes; else echo No;fi`

# Añade el campo de reporte ClamAV.
:0fw
| formail -i "X-Virus: $VIRUS"

# Si el mensaje es positivo a virus, se cambia el asunto.
:0fw
* ^X-Virus: Yes
| formail -i "Virus: $AV_REPORT" -i "Subject: MENSAJE CON VIRUS: $AV_REPORT"

# Hacer pasar todo el correo electrónico a través de spamassassin
:0fw
| /usr/bin/spamassassin
```

Con lo anterior, en adelante todo el correo será examinado primero por **ClamAV** y **Spamassassin** y clasificado antes de ser entregado al usuario. Es innecesario reiniciar el servicio **sendmail** o servicio alguno. Esta solución es perfecta para servidores de correo electrónico con **poco carga de trabajo**.

Si se tiene un servidor de correo electrónico con mucha carga de trabajo, instale el paquete clamav-scanner-sysvinit:

```
yum -y install clamav-scanner-sysvinit
```

Inicie el servicio clamd.scan, ejecutando lo siguiente:

```
service clamd.scan start
```

Inicie el servicio spamassassin, ejecutando lo siguiente.

```
service spamassassin start
```

Añada los servicios **clamd.scan** y **spamassassin**, al inicio del sistema:

```
chkconfig clamd.scan on
chkconfig spamassassin on
```

Genere un enlace simbólico como **/etc/clamd.conf**, que apunte hacia **/etc/clamd.d/scan.conf**:

```
ln -s /etc/clamd.d/scan.conf /etc/clamd.conf
```

Edite el archivo **/etc/procmailrc** y cambie **/usr/bin/clamscan** por **/usr/bin/clamdscan** y **/usr/bin/spamassassin** por **/usr/bin/spamc**.

```
SHELL=/bin/sh
# Si desea almacenar toda la información de actividad
# de Procmail en una bitácora, des-comente lo siguiente.
#LOGFILE=/var/log/procmail.log

# Configuración basada sobre http://bulma.net/body.phtml?nIdNoticia=1978
# y adecuada y actualizada, por Joel Barrios Dueñas.
AV_REPORT=`/usr/bin/clamdscan --stdout --no-summary - | cut -d: -f 2`
VIRUS=`if [ "$AV_REPORT" != " OK" ]; then echo Yes; else echo No;fi`

# Añade el campo de reporte ClamAV.
:0fw
| formail -i "X-Virus: $VIRUS"

# Si el mensaje es positivo a virus, se cambia el asunto.
:0fw
* ^X-Virus: Yes
| formail -i "Virus: $AV_REPORT" -i "Subject: MENSAJE CON VIRUS: $AV_REPORT"

# Hacer pasar todo el correo electrónico a través de spamassassin
:0fw
| /usr/bin/spamc
```

Con lo anterior, tendrá una solución aceptable, barata, confiable, rápida y sencilla, para servidores de correo electrónico **con mucha carga de trabajo**.

Si, además, necesita que todos los mensajes de Spam y los mensajes infectados con virus sean movidos automáticamente a la carpeta de correo **~/mail/Junk**, utilice la siguiente configuración para el archivo **/etc/procmailrc**:

```
SHELL=/bin/sh
# Si desea almacenar toda la información de actividad
# de Procmail en una bitácora, descomente lo siguiente.
#LOGFILE=/var/log/procmail.log

# Configuración basada sobre http://bulma.net/body.phtml?nIdNoticia=1978
# y adecuada y actualizada, por Joel Barrios Dueñas.
AV_REPORT=`/usr/bin/clamdscan --stdout --no-summary - | cut -d: -f 2`
VIRUS=`if [ "$AV_REPORT" != " OK" ]; then echo Yes; else echo No;fi`

# Añade el campo de reporte ClamAV.
:0fw
| formail -i "X-Virus: $VIRUS"

# Si el mensaje es positivo a virus, se cambia el asunto.
:0fw
* ^X-Virus: Yes
| formail -i "Virus: $AV_REPORT" -i "Subject: MENSAJE CON VIRUS: $AV_REPORT"

# Si el mensaje es positivo a virus, se almacena en $HOME/mail/Junk
:0:
* ^X-Virus: Yes
$HOME/mail/Junk
# Si lo desea, puede enviar los mensajes infectados a /dev/null.

# Hacer pasar todo el correo electrónico a través de spamassassin
:0fw
| /usr/bin/spamc

# Los mensajes marcados como spam, se almacenan en $HOME/mail/Junk
:0:
* ^X-Spam-Status: Yes
$HOME/mail/Junk
```

Si lo desea, puede descargar una copia del archivo **/etc/procmailrc** desde AlcanceLibre.org, con el contenido anterior.

```
wget http://www.alcancelibre.org/linux/secrets/procmailrc -O /etc/procmailrc
```

A fin de que todo lo anterior funcione correctamente, es imprescindible que los usuarios generen y se suscriban con antelación a la carpeta IMAP **$HOME/mail/Junk**. Es importante mencionar que con el primer mensaje que sea procesado, la carpeta IMAP **$HOME/mail/Junk** será propiedad de root, con permiso de sólo lectura para root, salvo que haya sido creada y suscrita previamente por el usuario.

Para automatizar lo anterior para las cuentas de usuario que sean creadas en lo subsecuente, ejecute lo siguiente para que /etc/skel incluya el archivo **~/mail/Junk** y para que la carpeta IMAP correspondiente esté suscrita de modo predeterminado.

```
mkdir -m 700 /etc/skel/mail
touch /etc/skel/mail/Junk
chmod 600 /etc/skel/mail/Junk
echo "Junk" > /etc/skel/mail/.subscriptions
chmod 600 /etc/skel/mail/.subscriptions
```

Si desea ahorrarse trabajo y explicaciones a los usuarios existentes, puede ejecutar lo siguiente:

```
cd /home
for user in *
do
mkdir -m 700 $user/mail
touch $user/mail/Junk
chmod 600 $user/mail/Junk
echo "Junk" >> $user/mail/.subscriptions
chmod 600 $user/mail/.subscriptions
chown -R $user:$user $user/mail/
done
cd -
```

Si tiene interés en mejorar y optimizar, el filtrado de *spam*, consulte el documento titulado «**Cómo instalar y configurar Spamassassin**.»

60. Introducción a los protocolos de correo electrónico.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

60.1. Introducción.

60.1.1. Preparativos.

A fin de poder realizar todas las pruebas correspondientes a cada protocolo, instale con el mandato **yum** los paquetes **netcat** (**nc**), **dovecot** y **postfix** o bien **sendmail**.

Si elige utilizar **sendmail**, ejecute lo siguiente:

```
yum -y install mailx nc dovecot sendmail
```

Si elige utilizar **postfix**, ejecute lo siguiente:

```
yum -y install mailx nc dovecot postfix
```

Si utiliza **CentOS 5** o **Red Hat Enterprise Linux 5**, omita el siguiente paso. Si utiliza **CentOS 6** o **Red Hat Enterprise Linux 6**, edite el archivo **/etc/dovecot/conf.d/10-mail.conf**:

```
vim /etc/dovecot/conf.d/10-mail.conf
```

Alrededor de la línea 30 del archivo **/etc/dovecot/conf.d/10-mail.conf**, establezca **mbox:~/mail:INBOX=/var/mail/%u** como valor de la opción **mail_location**.

```
# See doc/wiki/Variables.txt for full list. Some examples:
#
#   mail_location = maildir:~/Maildir
#   mail_location = mbox:~/mail:INBOX=/var/mail/%u
#   mail_location = mbox:/var/mail/%d/%1n/%n:INDEX=/var/indexes/%d/%1n/%n
#
# <doc/wiki/MailLocation.txt>
#
mail_location = mbox:~/mail:INBOX=/var/mail/%u
```

Si se va a utilizar Sendmail como MTA predeterminado, es importante definir un grupo de acceso de correo en la configuración de Dovecot. Si se va a utilizar Postfix se puede omitir los dos siguientes pasos.

Alrededor de la línea 115 del archivo **/etc/dovecot/conf.d/10-mail.conf**, localice la opción **mail_privileged_group**, descomente ésta y defina como valor el grupo **mail**:

```
# Group to enable temporarily for privileged operations. Currently this is
# used only with INBOX when either its initial creation or dotlocking fails.
# Typically this is set to "mail" to give access to /var/mail.
mail_privileged_group = mail
```

Alrededor de la línea 122 del archivo **/etc/dovecot/conf.d/10-mail.conf**, localice la opción **mail_access_groups**, descomente ésta y defina también como valor el grupo **mail**:

```
# Grant access to these supplementary groups for mail processes. Typically
# these are used to set up access to shared mailboxes. Note that it may be
# dangerous to set these if users can create symlinks (e.g. if "mail" group is
# set here, ln -s /var/mail ~/mail/var could allow a user to delete others'
# mailboxes, or ln -s /secret/shared/box ~/mail/mybox would allow reading it).
mail_access_groups = mail
```

Se requiere que los usuarios locales pertenezcan al grupo **mail** para que lo anterior represente un problema de seguridad.

Nota.

Es importante señalar Postfix crea automáticamente los buzones de entrada con permiso **0600** (-rw-------) y por tanto impide utilizar buzones de entrada compartidos, mientras que Sendmail lo hace con permiso **0660** (-rw-rw----) y por tanto permite utilizar buzones de entrada compartidos. En ambos casos los permisos predeterminados de los buzones de entrada sólo se pueden cambiar modificando y compilando de nuevo el código fuente.

Si se utiliza Sendmail como MTA predeterminado, debido al permiso **0660** con el que son creados los buzones de entrada, a Dovecot le será imposible generar automáticamente las carpetas e índices IMAP, pues éste fallará al copiar el grupo al que pertenece el buzón de entrada cuando éste tiene permisos de lectura y escritura para grupo. Por lo tanto se obtendrían continuamente los siguientes errores en la bitácora **/var/log/maillog**:

```
Mar 21 22:31:45 mail dovecot: pop3(fulano): Error: mkdir(/home/fulano/mail/.imap/INBOX) failed:
Operation not permitted
Mar 21 22:31:45 mail dovecot: pop3(fulano): Error: Couldn't open INBOX: Internal error occurred. Refer
to server log for more information. [2013-03-21 22:31:45]
Mar 21 22:31:45 mail dovecot: pop3(fulano): Couldn't open INBOX top=0/0, retr=0/0, del=0/0, size=0
```

Es por ésto que, en el caso de utilizar Sendmail como MTA predeterminado, se requiere configurar que Dovecot tenga privilegios de acceso sobre el grupo **mail**. De otro modo el administrador del sistema estaría obligado a crear manualmente los directorios ~/mail/.imap/INBOX de todos los usuarios locales o cambiar manualmente los permisos de todos los buzones de entrada de 0660 a 0600 y repetir cualquiera de las dos operaciones cada vez que se genere un nuevo usuario.

Si se utiliza Postfix como MTA predeterminado, es innecesario definir valor alguno en las opciones **mail_privileged_group** y **mail_access_groups** pues los buzones de entrada se crean con permiso **0600** y por tanto carecen de permisos de lectura y escritura para grupo.

Guarde el archivo y salga del editor de texto.

Inicie y active el servicio **dovecot** ejecutando:

```
service dovecot start
chkconfig dovecot on
```

Establezca **sendmail** o **postfix**, como agente de transporte de correo (**MTA**, **M**ail **T**ransport **A**gent) predeterminado del sistema, utilizando el mandato **alternatives**, del siguiente modo:

```
alternatives --config mta
```

Lo anterior devolverá una salida similar a la siguiente, donde deberá elegir entre **postfix** y **sendmail** como MTA predeterminado del sistema:

```
Hay 2 programas que proporcionan 'mta'.

  Selección    Comando
-----------------------------------------------
   1           /usr/sbin/sendmail.postfix
*+ 2           /usr/sbin/sendmail.sendmail

Presione Intro para mantener la selección actual[+] o escriba el número de la selección:  2
```

Si eligió utilizar **sendmail** en lugar de **postfix**, detenga este último (es el MTA predeterminado en **CentOS 6** y **Red Hat Enterprise Linux 6**) e inicie el servicio **sendmail**:

```
service postfix stop
chkconfig postfix off
service sendmail start
chkconfig sendmail on
```

Si eligió utilizar **postfix** en lugar de **sendmail**, detenga este último> (es el MTA predeterminado en **CentOS 5** y **Red Hat Enterprise Linux 5**) e inicie el servicio **postfix**:

```
service sendmail stop
chkconfig sendmail off
service postfix start
chkconfig postfix on
```

En todo momento podrá conmutar de nuevo entre Sendmail o Postfix, como MTA predeterminado del sistema, utilizando este mismo procedimiento.

60.1.2. Protocolos utilizados.

60.1.2.1. SMTP (Simple Mail Transfer Protocol).

Es un **protocolo estándar** de Internet, del **Nivel de Aplicación** utilizado, para la transmisión de correo electrónico a través de una conexión TCP/IP. Éste es, de hecho, el único protocolo utilizado para la transmisión de correo electrónico a través de Internet. Es un protocolo basado sobre texto y relativamente simple, donde se especifica un destinatario o múltiples destinatarios, en un mensaje que es transferido. A lo largo de los años han sido muchas las personas que han editado o contribuido a las especificaciones de **SMTP**, entre las cuales están Jon Postel, Eric Allman, Dave Crocker, Ned Freed, Randall Gellens, John Klensin y Keith Moore.

Para determinar el servidor **SMTP** para un dominio dado, se utilizan los registros **MX** (**M**ail E**x**changer) en la Zona de Autoridad correspondiente al ese mismo dominio contestado por un **Servidor DNS**. Después de establecerse una conexión entre el remitente (el cliente) y el destinatario (el servidor), se inicia una sesión **SMTP**, ejemplificada a continuación.

```
 Cliente: $ nc 127.0.0.1 25
Servidor: Trying 127.0.0.1...
          Connected to localhost.localdomain (127.0.0.1).
          Escape character is '^]'.
          220 nombre.dominio ESMTP Sendmail 8.13.1/8.13.1; Sat, 18 Mar 2006 16:02:27 -0600
 Cliente: HELO localhost.localdomain
Servidor: 250 nombre.dominio Hello localhost.localdomain [127.0.0.1], pleased to meet you
 Cliente: MAIL FROM:<fulano@localhost.localdomain>
Servidor: 250 2.1.0 <fulano@localhost.localdomain>... Sender ok
 Cliente: RCPT TO:<fulano@localhost.localdomain>
Servidor: 250 2.1.5 <fulano@localhost.localdomain>... Recipient ok
 Cliente: DATA
Servidor: 354 Enter mail, end with "." on a line by itself
 Cliente: Subject: Mensaje de prueba
          From: fulano@localhost.localdomain
          To: fulano@localhost.localdomain

          Hola. Éste es un mensaje de prueba.
          Adios.
          .
Servidor: 250 2.0.0 k2IM2RjA003987 Message accepted for delivery
 Cliente: QUIT
Servidor: 221 2.0.0 nombre.dominio closing connection
Servidor: Connection closed by foreign host.
```

La descripción completa del protocolo original **STMP** está definida en el **RFC 821**, aunque el protocolo utilizado hoy en día, también conocido como **ESMTP** (**E**xtended **S**imple **M**ail **T**ransfer **P**rotocol), está definido en el **RFC 2821**. **SMTP** trabaja sobre **TCP** en el puerto 25.

60.1.2.2. POP3 (Post Office Protocol version 3).

Es un **protocolo estándar** de Internet, del **Nivel de Aplicación**, que recupera el correo electrónico desde un servidor remoto a través de una conexión TCP/IP desde un cliente local. El diseño de **POP3** y sus predecesores es permitir a los usuarios recuperar el correo electrónico, mientras están conectados en una red y manipular los mensajes recuperados sin necesidad de permanecer conectados. A pesar de que muchos clientes de correo electrónico incluyen soporte para dejar el correo en el servidor, todos los clientes de POP3 recuperan todos los mensajes y los almacenan como **mensajes nuevos** en la computadora o anfitrión, utilizado por el usuario, eliminan los mensajes en el servidor y terminan la conexión.

Después de establecerse una conexión entre el cliente y el servidor, se inicia una sesión **POP3**, ejemplificada a continuación.

```
 Cliente: $ nc 127.0.0.1 110
Servidor: Trying 127.0.0.1...
          Connected to localhost.localdomain (127.0.0.1).
          Escape character is '^]'.
          +OK dovecot ready.
 Cliente: USER fulano
Servidor: +OK
 Cliente: PASS clave de accceso
Servidor: +OK Logged in.
 Cliente: STAT
Servidor: +OK 1 728
 Cliente: LIST
Servidor: +OK 1 messages:
          1 728
          .
 Cliente: RETR 1
Servidor: +OK 728 octets
          Return-Path: <fulano@localhost.localdomain>
          Received: from localhost.localdomain (localhost.localdomain [192.168.1.254])
                   by localhost.localdomain (8.13.1/8.13.1) with SMTP id k2IM2RjA003987
                   for <fulano@localhost.localdomain>; Sat, 18 Mar 2006 16:03:21 -0600
          Date: Sat, 18 Mar 2006 16:02:27 -0600
          Message-Id: <200603182203.k2IM2RjA003987@localhost.localdomain>
          Subject: Mensaje de prueba
          From: fulano@localhost.localdomain
          To: fulano@localhost.localdomain
          Status: O
          Content-Length: 43
          Lines: 2
          X-UID: 202
          X-Keywords:

          Hola. Éste es un mensaje de prueba.
          Adios.
          .
 Cliente: QUIT
Servidor: +OK Logging out.
          Connection closed by foreign host.
```

POP3 está definido en el **RFC 1939**. **POP3** trabaja sobre **TCP** en el puerto 110.

60.1.2.3. IMAP (Internet Message Access Protocol).

Es un **protocolo estándar** de Internet, del **Nivel de Aplicación**, utilizado para acceder hacia el correo electrónico almacenado en un servidor remoto, a través de una conexión TCP/IP desde un cliente local.

La versión más reciente de **IMAP** es la 4, revisión 1 y está definida en el **RFC 3501**. **IMAP** trabaja sobre **TCP** en el puerto 143.

Fue diseñado por Mark Crispin en 1986 como una alternativa más moderna que resolviera las deficiencias del protocolo **POP3**. Las características más importantes de **IMAP** incluyen:

- Soporte para los modos de operación conectado (connected) y desconectado (disconnected), permitiendo a los clientes de correo electrónico permanezcan conectados el mismo tiempo que su interfaz permanezca activa, descargando los mensajes, por partes o completos, conforme se necesite.
- A diferencia de **POP3**, permite accesos simultáneos desde múltiples clientes y proporciona los mecanismos necesarios para que éstos detecten los cambios hechos por otro cliente de correo electrónico que esté conectado de manera concurrente al mismo buzón de correo.

- Permite a los clientes obtener individualmente cualquier parte **MIME** (acrónimo de **M**ulti-Purpose **I**nternet **M**ail **E**xtensions o Extensiones de correo de Internet de propósitos múltiples), así como también obtener porciones de las partes individuales o bien los mensajes completos.
- A través de **banderas** definidas en el protocolo, permite vigilar la información de estado de los mensajes de correo electrónico que se mantengan en el servidor. Por ejemplo, si el estado del mensaje es **leído**, **no leído**, **respondido** o **eliminado**.
- Incluye soporte para múltiples buzones de correo electrónico, permitiendo crear, renombrar o eliminar, mensajes de correo electrónico presentes en el servidor dentro de carpetas y mover estos mensajes entre distintas cuentas de correo electrónico. Esta característica también permite al servidor proporcionar acceso hacia los carpetas públicas y las compartidas.
- Incluye soporte para realizar búsquedas del lado del servidor a través de mecanismos que permiten obtener resultados de acuerdo a varios criterios, permitiendo evitar que los clientes de correo electrónico tengan que descargar todos los mensajes desde el servidor.
- Las especificaciones del protocolo **IMAP** definen un mecanismo explícito mediante el cual puede ser mejorada su funcionalidad a través de extensiones. Un ejemplo es la extensión **IMAP IDLE**, la cual permite sincronizar ente el servidor y el cliente a través de avisos.

Después de establecerse una conexión entre el cliente y el servidor, se inicia una sesión **IMAP**, ejemplificada a continuación.

```
 Cliente: $ nc 127.0.0.1 143
Servidor: Trying 127.0.0.1...
          Connected to localhost.localdomain (127.0.0.1).
          Escape character is '^]'.
          * OK dovecot ready.
          +OK dovecot ready.
 Cliente: x LOGIN fulano clave de acceso
Servidor: x OK Logged in.
 Cliente: x SELECT inbox
Servidor: * FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
          * OK [PERMANENTFLAGS (\Answered \Flagged \Deleted \Seen \Draft \*)] Flags permitted.
          * 1 EXISTS
          * 0 RECENT
          * OK [UNSEEN 1] First unseen.
          * OK [UIDVALIDITY 1100569382] UIDs valid
          * OK [UIDNEXT 203] Predicted next UID
          x OK [READ-WRITE] Select completed.
 Cliente: x FETCH 1 (flags body[header.fields (subject)])
Servidor: * 1 FETCH (FLAGS (\Seen) BODY[HEADER.FIELDS (SUBJECT)] {30}
          Subject: Mensaje de prueba

          )
          x OK Fetch completed.
          .
 Cliente: x FETCH 1 (body[text])
Servidor: * 1 FETCH (BODY[TEXT] {45}
          Hola. Éste es un mensaje de prueba.
          Adios.
          )
          x OK Fetch completed.
 Cliente: x LOGOUT
Servidor: * BYE Logging out
          x OK Logout completed.
          Connection closed by foreign host.
```

60.2. Referencias.

http://www.ietf.org/rfc/rfc2222.txt
http://www.ietf.org/rfc/rfc821.txt
http://www.ietf.org/rfc/rfc2821.txt
http://www.ietf.org/rfc/rfc1939.txt
http://www.ietf.org/rfc/rfc3501.txt

61. Configuración básica de Sendmail.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

61.1. Introducción.

Es imprescindible primero estudiar y comprender, los conceptos descritos en el documento titulado «**Introducción a los protocolos de correo electrónico**.»

61.1.1. Acerca de Sendmail.

Es el más popular agente de transporte de correo (MTA o **M**ail **T**ransport **A**gent), responsable, quizá, de poco más del 70% del correo electrónico del mundo. Aunque por largo tiempo se le ha criticado por muchos incidentes de seguridad, lo cierto es que éstos siempre han sido resueltos en pocas horas.

URL: http://www.sendmail.org/.

61.1.2. Acerca de Dovecot.

Dovecot es un servidor de POP3 e IMAP, de código fuente abierto, que funciona en Linux y sistemas basados sobre Unix™ y diseñado con la seguridad como principal objetivo. **Dovecot** puede utilizar tanto el formato **mbox** como **maildir** y es compatible con las implementaciones de los servidores UW-IMAP y Courier IMAP.

URL: http://dovecot.procontrol.fi/.

61.1.3. Acerca de SASL y Cyrus SASL.

SASL (**S**imple **A**uthentication and **S**ecurity **L**ayer) es una implementación diseñada para la seguridad de datos en protocolos de Internet. Desempareja los mecanismos de la autenticación desde protocolos de aplicaciones, permitiendo, en teoría, cualquier mecanismo de autenticación soportado por SASL, para ser utilizado en cualquier protocolo de aplicación que sea capaz de utilizar SASL. Actualmente SASL es un protocolo de la IETF (**I**nternet **E**ngineering **T**ask **F**orce) que ha sido propuesto como estándar. Está especificado en el **RFC 2222** creado por John Meyers en la Universidad Carnegie Mellon.

Cyrus SASL es una implementación de **SASL** que puede ser utilizada del lado del servidor o bien del lado del cliente y que incluye como principales mecanismos de autenticación soportados a ANONYMOUS, CRAM-MD5, DIGEST-MD5, GSSAPI y PLAIN. El código fuente incluye también soporte para los mecanismos LOGIN, SRP, NTLM, OPT y KERBEROS_V4.

URL: http://asg.web.cmu.edu/sasl/sasl-library.html.

61.2. Equipamiento lógico necesario.

- cyrus-sasl
- cyrus-sasl-plain
- dovecot
- m4
- make
- sendmail-cf
- sendmail

Instalación a través de yum.

Si se utiliza de **CentOS** o **Red Hat Enterprise Linux** ejecute lo siguiente:

```
yum -y install sendmail sendmail-cf dovecot m4 make \
    cyrus-sasl cyrus-sasl-plain
```

Si acaso estuviese instalado, elimine el paquete cyrus-sasl-gssapi, ya que este utiliza el método de autenticación GSSAPI, mismo que requeriría de la base de datos de cuentas de usuario de un servidor Kerberos. De igual manera, si estuviese instalado, elimine el paquete cyrus-sasl-md5, ya que este utiliza los métodos de autenticación CRAM-MD5 y Digest-MD5, mismos que requerían asignar las contraseñas para SMTP a través del mandato saslpasswd2. Outlook carece de soporte para estos métodos de autenticación.

```
yum remove cyrus-sasl-gssapi cyrus-sasl-md5
```

61.3. Procedimientos.

61.3.1. Definiendo Sendmail como agente de transporte de correo predeterminado.

El mandato **alternatives**, con la opción **--config** y el valor **mta**, se utiliza para conmutar el servicio de correo electrónico del sistema y elegir qué programa utilizar. Sólo es necesario utilizar éste si previamente estaban instalados Postfix o Exim. Sí este es el caso, ejecute lo siguiente desde una terminal y defina **Sendmail** como agente de transporte de correo (**MTA**, **M**ail **T**ransport **A**gent), seleccionado éste.

```
alternatives --config mta
```

Lo anterior devolverá una salida similar a la siguiente, donde deberá elegir entre **postfix** y **sendmail** como MTA predeterminado del sistema:

```

Hay 2 programas que proporcionan 'mta'.

  Selección    Comando
-----------------------------------------------
   1           /usr/sbin/sendmail.postfix
*+ 2           /usr/sbin/sendmail.sendmail

Presione Intro para mantener la selección actual[+] o bien escriba el número de la selección:  2
```

Si estuviera presente **postfix**, detenga éste (es el **MTA** predeterminado en **CentOS 6** y **Red Hat Enterprise Linux 6**) e inicie el servicio **sendmail**:

```
service postfix stop
chkconfig postfix off
service sendmail start
chkconfig sendmail on
```

61.3.2. Alta de cuentas de usuario y asignación de contraseñas.

La autenticación para **SMTP**, a través de cualquier método (**PLAIN**, **LOGIN**, **Digest-MD5** o **CRAM-MD5**), requiere se active, e inicie, el servicio **saslauthd** del siguiente modo:

```
chkconfig saslauthd on
service saslauthd start
```

El alta de usuarios es la misma que como con cualquier otro usuario del sistema. Sendmail utilizará el servicio **saslauthd** para autenticar a los usuarios a través de los métodos **PLAIN** y **LOGIN**, con opción a utilizar también **Digest-MD5** o bien **CRAM-MD5**.

El alta de las cuentas del usuario en el sistema, la cual se sugiere se asigne **/dev/null** o **/sbin/nologin** como intérprete de mandatos, pude hacerse del siguiente modo:

```
useradd -s /dev/null usuario
```

La asignación de contraseñas, para permitir autenticar a través de **SMTP**, **POP3**, e **IMAP**, utilizando el método **PLAIN** o bien el método **LOGIN**, se hace exactamente igual que con cualquier otra cuenta de usuario del sistema, como se muestra a continuación:

```
passwd usuario
```

Ejecutando lo anterior, el sistema solicitará se ingrese una contraseña, con confirmación. Prefiera utilizar buenas contraseñas y de este modo evitará problemas de seguridad.

Nota.

La asignación de contraseñas para autenticar **SMTP**, a través de métodos cifrados (**CRAM-MD5** y **DIGEST-MD5**), en sistemas con versión de Sendmail compilada contra **SASL-2** (Red Hat™ Enterprise Linux 5, CentOS 5 y versiones posteriores de éstos), puede hacerse a través del mandato **saslpasswd2** del siguiente modo, tomando en consideración que **Outlook y Outlook Express carecen de soporte para autenticar contraseñas a través de estos métodos, los cuales requieren además tener instalado el paquete cyrus-sasl-md5 en el servidor para la gestión de contraseñas**:

```
saslpasswd2 usuario
```

Puede mostrarse la lista de los usuarios con contraseña asignada a través de SASL-2 utilizando el mandato **sasldblistusers2**.

Si los usuarios se van a dar de alta siguiendo el formato *usuario@dominio.tld* en lugar de sólo *usuario*, una práctica común en los servidores con múltiples dominios virtuales, es necesario añadir al servicio **saslauthd** la opción **-r**, la cual permite combinar el nombre de usuario y dominio antes de pasar por el mecanismo de autenticación. Si éste es el caso, se debe editar el archivo **/etc/sysconfig/saslauthd**:

```
vi /etc/sysconfig/saslauthd
```

Y añadir la opción **-r** a los argumentos de **FLAGS**:

```
# Directory in which to place saslauthd's listening socket, pid file, and so
# on.  This directory must already exist.
SOCKETDIR=/var/run/saslauthd

# Mechanism to use when checking passwords.  Run "saslauthd -v" to get a list
# of which mechanism your installation was compiled with the ablity to use.
MECH=pam

# Options sent to the saslauthd. If the MECH is other than "pam" uncomment
# the next line.
# DAEMONOPTS=--user saslauth

# Additional flags to pass to saslauthd on the command line.  See saslauthd(8)
# for the list of accepted flags.
FLAGS=-r
```

Y reiniciar el servicio **saslauthd**.

```
service saslauthd restart
```

61.3.3. Dominios a administrar.

Edite el archivo **/etc/mail/local-host-names**:

```
vi /etc/mail/local-host-names
```

Establezca los dominios locales que serán administrados. En el siguiente ejemplo se establecen 4 dominios a administrar, donde **tld** (***T**op **L**evel **D**omain* o dominio de nivel superior) correspondería a .com, .org, .net, etc.:

```
dominio1.tld
dominio2.tld
dominio3.tld
dominio4.tld
```

Proceda a crear el archivo **/etc/mail/relay-domains**:

```
touch /etc/mail/relay-domains
```

Edite el archivo **/etc/mail/relay-domains** que acaba de crear:

```
vi /etc/mail/relay-domains
```

Establezca los nombres de los dominios que tendrán permitido re-transmitir correo electrónico desde el servidor. Técnicamente tendrá **casi** el mismo contenido de **/etc/mail/local-host-names**, a menos que se desee excluir algún dominio en particular o bien se trate de servidor de correo secundario para otro dominio en otro servidor.

```
dominio1.tld
dominio2.tld
dominio3.tld
dominio4.tld
```

61.3.4. Control de acceso

Para definir las listas de control de acceso, edite el archivo **/etc/mail/access**:

```
vi /etc/mail/access
```

Debe incluir en el archivo **/etc/mail/access** todas **las direcciones IP locales del servidor** (las que devuelva el mandato **ip addr show**).

Puede incluir también la lista direcciones IP, dominios o bien cuentas de correo electrónico, a las que se quiera otorgar permisos de re-transmisión sin restricciones o con permiso para enviar correo electrónico sólo a cuentas locales. Puede definir también una *lista negra* de direcciones de correo electrónico, dominios y direcciones IP, a las que se desee denegar el acceso. Considere que:

- Cualquier elemento que vaya acompañado de **RELAY**, tendrá permitido enviar correo electrónico, sin necesidad de autenticar y **re-transmitir** éste **sin restricción alguna**.
- Cualquier elemento que vaya acompañado de **OK**, tendrá permitido enviar correo electrónico, sin necesidad de autenticar, pero sólo a las cuentas locales.
- Cualquier elemento que vaya acompañado de **REJECT**, tendrá prohibida cualquier tipo de comunicación de correo electrónico.

Nota.

Jamás configure una segmento completo de red local con RELAY, ya que dejaría de tener sentido utilizar autenticación a través de SMTP y potencialmente podría permitir que los problemas de seguridad de maquinas infectadas con virus, gusanos o troyanos, se magnifiquen, siendo que permitiría el envío, **sin restricciones**, de correo electrónico infectado o bien cantidades extraordinarias de *spam*, originadas por los equipos cuya seguridad se haya visto comprometida.

Ejemplo de configuración para el archivo **/etc/mail/access**:

```
Connect:localhost.localdomain   RELAY
Connect:localhost               RELAY
Connect:127.0.0.1               RELAY
#
# Dirección IP del propio servidor.
Connect:192.168.70.51           RELAY
#
# Otros servidores de correo en la LAN a los que se les permitirá enviar
# correo libremente a través del propio servidor de correo.
Connect:192.168.70.52           RELAY
#
# Direcciones IP que sólo podrán entregar correo de forma local, es decir,
# no pueden enviar correo fuera del propio servidor.
Connect:192.168.2.24            OK
#
# Lista negra
usuario@molesto.com     REJECT
productoinutil.com.mx   REJECT
10.4.5.6                REJECT
#
# Bloques de Asia Pacific Networks, ISP desde el cual se emite la mayor
# parte del Spam del mundo.
# Las redes involucradas abarcan Australia, Japón, China, Corea del Sur,
Taiwan,
# Hong Kong e India por lo que bloquear el correo de dichas redes significa
# cortar comunicación con estos países, pero acaba con entre el 60% y 80%
# del Spam.
222                     REJECT
221                     REJECT
220                     REJECT
219                     REJECT
218                     REJECT
212                     REJECT
211                     REJECT
210                     REJECT
203                     REJECT
202                     REJECT
140.109                 REJECT
133                     REJECT
61                      REJECT
60                      REJECT
59                      REJECT
58                      REJECT
```

61.3.5. Alias de la cuenta del usuario root.

Es peligroso autenticarse con la cuenta del usuario **root**, a través de cualquier tipo de red, sólo para revisar los mensajes de correo electrónico originados por el sistema. Se recomienda definir alias para la cuenta del usuario **root**, hacia la cual se entregará todo el correo electrónico originalmente dirigido a root.

Edite el archivo **/etc/aliases**:

```
vi /etc/aliases
```

Al final de éste, defina a que cuenta de usuario regular le será entregado el correo electrónico originalmente destinado a root:

```
root:           fulano
```

Para convertir el archivo /etc/aliases en /etc/aliases.db, que es el archivo, en formato de base de datos, que utilizará sendmail y para verificar que la sintaxis esté correcta o bien si existen aliases duplicados, ejecute el siguiente mandato:

```
newaliases
```

Lo anterior, debe devolver una salida similar a la siguiente:

```
/etc/aliases: 77 aliases, longest 10 bytes, 777 bytes total
```

61.3.6. Configuración de funciones de Sendmail.

Para definir, cambiar o añadir funciones, edite el archivo **/etc/mail/sendmail.mc**.

```
vi /etc/mail/sendmail.mc
```

61.3.6.1. confSMTP_LOGIN_MSG.

Este parámetro permite establecer el mensaje de bienvenida al establecer la conexión al servidor. Es posible ocultar el nombre y la versión de Sendmail, ésto con el objeto de agregar *seguridad por oscuridad*. Funciona de manera sencilla, haciendo que, quien establezca una conexión hacia el servidor, sea incapaz determinar qué versión de Sendmail se está utilizando y con ésto dificultar a un delincuente o abusador del servicio, el determinar que vulnerabilidad específica aprovechar. Descomente lo siguiente en el archivo **/etc/mail/sendmail.mc**, eliminando el **dnl** y el espacio que le antecede:

```
dnl #
dnl # Do not advertize sendmail version.
dnl #
define(`confSMTP_LOGIN_MSG',`$j Sendmail; $b')dnl
dnl #
dnl # default logging level is 9, you might want to set it higher to
dnl # debug the configuration
dnl #
dnl define(`confLOG_LEVEL', `9')dnl
```

Guarde los cambios y salga del editor.

Reinicie el servicio **sendmail**:

```
service sendmail restart
```

Realice una conexión al puerto 25. Obtendrá una salida similar a la siguiente:

```
$ nc 127.0.0.1 25
Trying 127.0.0.1...
Connected to mail.dominio.tld.
Escape character is '^]'.
220 mail.dominio.tld ESMTP Sendmail ; Mon, 17 May 2004 02:22:29 -0500
quit
221 2.0.0 mail.dominio.tld closing connection
Connection closed by foreign host.
$
```

61.3.6.2. confAUTH_OPTIONS.

Vuelva a edita el archivo **/etc/mail/sendmail.mc**:

```
vi /etc/mail/sendmail.mc
```

La siguiente línea viene habilitada de modo predeterminado y permitirá realizar el proceso de autenticación a través del puerto 25, utilizando el método **PLAIN** o bien el método **LOGIN**, los cuales transmiten el nombre de usuario, junto con su correspondiente contraseña, en texto simple, garantizando 100% de compatibilidad con todos los clientes de correo electrónico existentes. Sin embargo, ésto también implica un enorme riesgo de seguridad, por lo cual se recomienda implementar seguridad a través de SSL/TLS.

```
define(`UUCP_MAILER_MAX', `2000000')dnl
define(`confUSERDB_SPEC', `/etc/mail/userdb.db')dnl
define(`confPRIVACY_FLAGS', `authwarnings,novrfy,noexpn,restrictqrun')dnl
define(`confAUTH_OPTIONS',`A')dnl
dnl #
dnl # The following allows relaying if the user authenticates, and disallows
dnl # plaintext authentication (PLAIN/LOGIN) on non-TLS links
```

Para añadir la seguridad necesaria, consulte y estudie el documento titulado «**Cómo configurar Sendmail y Dovecot con soporte SSL/TLS**.»

.

Nota.

Si utiliza la siguiente línea, en lugar de la mencionada arriba, se desactivará la función que permite la autenticación enviando las contraseñas en texto simple, a través de conexiones sin cifrar (SSL/TLS) y se habilitará la función que sólo permite autenticar con contraseñas en texto simple a través de SSL/TLS y a través de métodos que utilicen contraseñas cifradas, como sería CRAM-MD5 y DIGEST-MD5 con o sin SSL/TLS. **Esto obliga a utilizar SSL/TLS para realizar conexiones a través de cualquier cliente de correo electrónico o bien clientes de correo electrónico con soporte para autenticación a través de CRAM-MD5 y DIGEST-MD5**.

Todos clientes de correo electrónico conocidos, excepto Outlook y Outlook Express), incluyen soporte para CRAM-MD5 y DIGEST-MD5. Las conexiones sin SSL/TLS requieren a tener instalado el paquete **cyrus-sasl-md5** en el servidor y asignar las contraseñas para SMTP a través del mandato **saslpasswd2**.

```
dnl # The following allows relaying if the user authenticates, and disallows
dnl # plaintext authentication (PLAIN/LOGIN) on non-TLS links
dnl #
define(`confAUTH_OPTIONS',`A p')dnl
dnl #
dnl # PLAIN is the preferred plaintext authentication method and used by
dnl # Mozilla Mail and Evolution, though Outlook Express and other MUAs do
dnl # use LOGIN. Other mechanisms should be used if the connection is not
```

Conviene habilitar esta opción en lugar de la anterior una vez que se ha configurado el **soporte SSL/TLS para Sendmail**, pues obliga a los usuarios a autenticarse utilizando sólo conexiones SSL/TLS.

61.3.6.3. TRUST_AUTH_MECH y confAUTH_MECHANISMS.

Si se desea utilizar SMTP con autenticación, se requieren des-comentar las siguientes dos líneas del archivo **/etc/mail/sendmail.mc**, eliminando el **dnl** y el espacio que les precede:

```
dnl # PLAIN is the preferred plaintext authentication method and used by
dnl # Mozilla Mail and Evolution, though Outlook Express and other MUAs do
dnl # use LOGIN. Other mechanisms should be used if the connection is not
dnl # guaranteed secure.
dnl # Please remember that saslauthd needs to be running for AUTH.
dnl #
TRUST_AUTH_MECH(`EXTERNAL DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
define(`confAUTH_MECHANISMS', `EXTERNAL GSSAPI DIGEST-MD5 CRAM-MD5LOGIN PLAIN')dnl
dnl #
dnl # Rudimentary information on creating certificates for sendmail TLS:
dnl #     cd /etc/pki/tls/certs; make sendmail.pem
```

61.3.6.4. DAEMON_OPTIONS.

De modo predeterminado, **Sendmail** escucha peticiones sólo a través de la interfaz de retorno del sistema (127.0.0.1), e ignorando otros dispositivos de red. Sólo se necesita eliminar la restricción de la interfaz de retorno para poder recibir correo desde Internet o desde la red de área local. Localice la siguiente línea resaltada:

```
dnl # The following causes sendmail to only listen on the IPv4 loopback address
dnl # 127.0.0.1 and not on any other network devices. Remove the loopback
dnl # address restriction to accept email from the internet or intranet.
dnl #
DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')dnl
dnl #
dnl # The following causes sendmail to additionally listen to port 587 for
dnl # mail from MUAs that authenticate. Roaming users who can't reach their
dnl # preferred sendmail daemon due to port 25 being blocked or redirected find
dnl # this useful.
dnl #
DAEMON_OPTIONS(`Port=submission, Name=MSA, M=Ea')dnl
dnl #
dnl # The following causes sendmail to additionally listen to port 465, but
dnl # starting immediately in TLS mode upon connecting. Port 25 or 587 followed
```

Examine este parámetro y elimine el valor **Addr=127.0.0.1**, además de la coma (,) que le antecede, de modo que quede como se muestra a continuación:

```
dnl # The following causes sendmail to only listen on the IPv4 loopback address
dnl # 127.0.0.1 and not on any other network devices. Remove the loopback
dnl # address restriction to accept email from the internet or intranet.
dnl #
DAEMON_OPTIONS(`Port=smtp, Name=MTA')dnl
dnl #
dnl # The following causes sendmail to additionally listen to port 587 for
dnl # mail from MUAs that authenticate. Roaming users who can't reach their
dnl # preferred sendmail daemon due to port 25 being blocked or redirected find
dnl # this useful.
dnl #
DAEMON_OPTIONS(`Port=submission, Name=MSA, M=Ea')dnl
dnl #
dnl # The following causes sendmail to additionally listen to port 465, but
dnl # starting immediately in TLS mode upon connecting. Port 25 or 587 followed
```

El puerto 587 (submission) puede ser utilizado también para envío de correo electrónico. Por estándar se utiliza como puerto alternativo en los casos donde un cortafuegos impide a los usuarios acceder hacia servidores de correo electrónico, los cuales normalmente trabajan a través del puerto 25. Para este fin, se requiere descomentar la línea que incluye **DAEMON_OPTIONS(`Port=submission, Name=MSA, M=Ea')dnl**, como se ilustra a continuación, resaltado en **negrita**:

```
dnl # The following causes sendmail to only listen on the IPv4 loopback address
dnl # 127.0.0.1 and not on any other network devices. Remove the loopback
dnl # address restriction to accept email from the internet or intranet.
dnl #
DAEMON_OPTIONS(`Port=smtp, Name=MTA')dnl
dnl #
dnl # The following causes sendmail to additionally listen to port 587 for
dnl # mail from MUAs that authenticate. Roaming users who can't reach their
dnl # preferred sendmail daemon due to port 25 being blocked or redirected find
dnl # this useful.
dnl #
DAEMON_OPTIONS(`Port=submission, Name=MSA, M=Ea')dnl
dnl #
dnl # The following causes sendmail to additionally listen to port 465, but
dnl # starting immediately in TLS mode upon connecting. Port 25 or 587 followed
```

61.3.6.5. FEATURE(`accept_unresolvable_domains').

De modo predeterminado, como una forma de permitir el envío local del correo del propio sistema en una computadora de escritorio o una computadora portátil, está se utiliza el parámetro **FEATURE(`accept_unresolvable_domains')**. Se recomienda desactivar esta función a fin de impedir se acepte correo de dominios inexistentes (generalmente utilizado para el envío de correo masivo no solicitado o **Spam**). Comente esta línea colocando un **dnl** y un espacio, del siguiente modo:

```
dnl # We strongly recommend not accepting unresolvable domains if you want to
dnl # protect yourself from spam. However, the laptop and users on computers
dnl # that do not have 24x7 DNS do need this.
dnl #
dnl FEATURE(`accept_unresolvable_domains')dnl
dnl #
dnl FEATURE(`relay_based_on_MX')dnl
dnl #
```

61.3.6.6. Enmascaramiento.

Des-comente las siguientes tres líneas y adapte el valor de **MASQUERADE_AS** para definir la máscara que utilizará el servidor para enviar correo electrónico (es decir, define lo que va después de la @ en la dirección de correo):

```
MASQUERADE_AS(`dominio1.tld')dnl
FEATURE(masquerade_envelope)dnl
FEATURE(masquerade_entire_domain)dnl
```

Si se van a administrar múltiples dominios, añada aquellos deban conservar su propia máscara, utilizando el parámetro **MASQUERADE_EXCEPTION** del siguiente modo:

```
MASQUERADE_AS(`dominio1.tld')dnl
MASQUERADE_EXCEPTION(`dominio2.tld')dnl
MASQUERADE_EXCEPTION(`dominio3.tld')dnl
MASQUERADE_EXCEPTION(`dominio4.tld')dnl
FEATURE(masquerade_envelope)dnl
FEATURE(masquerade_entire_domain)dnl
```

61.3.6.7. Control del correo chatarra (spam) a través de DNSBLs.

Si se desea utilizar *listas negras* para mitigar el correo chatarra (*spam*), pueden añadir la siguiente línea para definir la lista negra de **SpamCop.net**, casi al final del archivo **/etc/mail/sendmail.mc** y justo arriba de *MAILER(smtp)dnl*:

```
dnl MASQUERADE_DOMAIN(localhost.localdomain)dnl
dnl MASQUERADE_DOMAIN(mydomainalias.com)dnl
dnl MASQUERADE_DOMAIN(mydomain.lan)dnl
FEATURE(`enhdnsbl', `bl.spamcop.net', `"Spam blocked see: http://spamcop.net/bl.shtml?"$&{client_addr}', `t')dnl
MAILER(smtp)dnl
MAILER(procmail)dnl
dnl MAILER(cyrusv2)dnl
```

61.3.7. Configuración de Dovecot.

61.3.7.1. Opciones del archivo /etc/dovecot/dovecot.conf en CentOS 6 y Red Hat Enterprise Linux 6.

CentOS 6 y **Red Hat Enterprise Linux 6** utilizan la versión **2.0** de **Dovecot** y por lo cual cambia radicalmente la configuración respecto de la versión **1.0.x**, utilizada en **CentOS 5** y **Red Hat Enterprise Linux 5** y versiones anteriores. Edite el archivo **/etc/dovecot/dovecot.conf** y descomente el parámetro **protocols**, estableciendo como valor **pop3 imap lmtp**.

```
# Protocols we want to be serving.
protocols = imap pop3 lmtp
```

61.3.7.2. Opciones del archivo /etc/dovecot/conf.d/10-mail.conf en CentOS 6 y Red Hat Enterprise Linux 6.

Alrededor de la línea 30 del archivo **/etc/dovecot/conf.d/10-mail.conf**, establezca **mbox:~/mail:INBOX=/var/mail/%u** como valor del parámetro **mail_location**.

```
# See doc/wiki/Variables.txt for full list. Some examples:
#
#   mail_location = maildir:~/Maildir
#   mail_location = mbox:~/mail:INBOX=/var/mail/%u
#   mail_location = mbox:/var/mail/%d/%1n/%n:INDEX=/var/indexes/%d/%1n/%n
#
# <doc/wiki/MailLocation.txt>
#
mail_location = mbox:~/mail:INBOX=/var/mail/%u
```

En este mismo archivo, alrededor de la línea 115, localice la opción **mail_privileged_group**, descomente ésta y defina como valor el grupo **mail**:

```
# Group to enable temporarily for privileged operations. Currently this is
# used only with INBOX when either its initial creation or dotlocking fails.
# Typically this is set to "mail" to give access to /var/mail.
mail_privileged_group = mail
```

Alrededor de la línea 122 del archivo **/etc/dovecot/conf.d/10-mail.conf**, localice la opción **mail_access_groups**, descomente ésta y defina también como valor el grupo **mail**:

```
# Grant access to these supplementary groups for mail processes. Typically
# these are used to set up access to shared mailboxes. Note that it may be
# dangerous to set these if users can create symlinks (e.g. if "mail" group is
# set here, ln -s /var/mail ~/mail/var could allow a user to delete others'
# mailboxes, or ln -s /secret/shared/box ~/mail/mybox would allow reading it).
mail_access_groups = mail
```

Se requiere que los usuarios locales pertenezcan al grupo **mail** para que lo anterior represente un problema de seguridad.

Cabe señalar que la versión de dovecot incluida en **CentOS 6** y **Red Hat™ Enterprise Linux 6**, es obligatorio generar un certificado, pues sólo permitirá conexiones sin TLS desde 127.0.0.1. Siga el procedimiento descrito en el documento titulado **Cómo configurar Sendmail y Dovecot con soporte SSL/TLS**.

61.3.7.3. Opciones del archivo /etc/dovecot/conf.d/10-auth.conf en CentOS 6 y Red Hat Enterprise Linux 6.

De modo predeterminado Dovecot sólo permite autenticar con texto simple sin SSL/TLS desde el anfitrión local. La autenticación de usuarios desde anfitriones remotos sólo se permite a través de SSL/TLS. Si requiere permitir la autenticación de usuarios sin SSL/TLS —**algo poco prudente en servidores en producción**, pero perfecto para realizar pruebas simples de autenticación— edite el archivo /etc/dovecot/conf.d/10-auth.conf:

```
vi /etc/dovecot/conf.d/10-auth.conf
```

Localice la opción **disable_plaintext_auth**:

```
##
## Authentication processes
##

# Disable LOGIN command and all other plaintext authentications unless
# SSL/TLS is used (LOGINDISABLED capability). Note that if the remote IP
# matches the local IP (ie. you're connecting from the same computer), the
# connection is considered secure and plaintext authentication is allowed.
#disable_plaintext_auth = yes
```

Quite la almohadilla y cambie el valor **yes** por **no**:

```
##
## Authentication processes
##

# Disable LOGIN command and all other plaintext authentications unless
# SSL/TLS is used (LOGINDISABLED capability). Note that if the remote IP
# matches the local IP (ie. you're connecting from the same computer), the
# connection is considered secure and plaintext authentication is allowed.
disable_plaintext_auth = no
```

Se recomienda dejar la opción **disable_plaintext_auth** con la opción **yes** a fin de obligar a los usuarios a autenticar sólo **a través de conexiones SSL/TLS**.

61.3.7.4. Opciones del archivo /etc/dovecot/dovecot.conf en CentOS 5 y Red Hat Enterprise Linux 5.

Si utiliza **CentOS 5** o **Red Hat™ Enterprise Linux 5**, sólo debe editar el archivo **/etc/dovecot.conf** y habilitar los servicios de IMAP y/o POP3, del siguiente modo (están habilitados de modo predeterminado pop3, pop3s, imap, e imaps):

```
# Protocols we want to be serving:
# imap imaps pop3 pop3s
protocols = imap imaps pop3 pop3s
```

61.3.8. Añadir al inicio del sistema e iniciar servicios dovecot y sendmail.

El servicio **dovecot**, en cualquiera de las versiones de los sistemas operativos mencionados, se agrega al inicio del sistema del siguiente modo:

```
chkconfig dovecot on
```

Para iniciar el servicio **dovecot**, se ejecuta lo siguiente:

```
service dovecot start
```

Para aplicar cambios en la configuración del servicio **dovecot**, se ejecuta lo siguiente:

```
service dovecot restart
```

El servicio **sendmail** se agrega al inicio del sistema, ejecutando lo siguiente:

```
chkconfig sendmail on
```

Para iniciar el servicio **sendmail**, se ejecuta lo siguiente:

```
service sendmail start
```

Para reiniciar servicio **sendmail**, sólo bastará ejecutar:

```
service sendmail restart
```

Probar servidor enviando/recibiendo mensajes con CUALQUIER cliente estándar de correo electrónico con soporte para POP3/IMAP/SMTP con soporte para autenticar a través de SMTP utilizando los métodos LOGIN o PLAIN.

Para detectar posibles errores, se puede examinar el contenido de la bitácora de correo electrónico del sistema, utilizando el mandato **tail**, con la opción **-f**, sobre el archivo **/var/log/maillog**, como se muestra a continuación:

```
tail -f /var/log/maillog
```

61.4. Modificaciones necesarias en el muro cortafuegos.

Como medida de seguridad, siempre abra los puertos del cortafuegos sólo hasta después de finalizar la configuración del servidor de correo electrónico y que sólo hasta que haya comprobado las configuraciones.

Para el funcionamiento normal de un servicio de correo electrónico estándar, es necesario abrir los puertos 25 (smtp), 465 (smtps), 587 (submission), 110 (pop3), 143 (imap), 993 (imaps) y 995 (pop3s), todos por TCP.

61.4.1. Servicio iptables.

Puede utilizar **iptables**, ejecutando lo siguiente:

```
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 25 -j ACCEPT
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 110 -j ACCEPT
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 143 -j ACCEPT
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 465 -j ACCEPT
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 587 -j ACCEPT
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 993 -j ACCEPT
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 995 -j ACCEPT
service iptables save
```

O bien añada lo siguiente al archivo **/etc/sysconfig/iptables**:

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 25 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 110 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 143 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 465 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 587 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 993 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 995 -j ACCEPT
```

Y reinicie el servicio **iptables**:

```
service iptables restart
```

61.4.2. Shorewall.

Edite el archivo **/etc/shorewall/rules**:

```
vi /etc/shorewall/rules
```

Las reglas corresponderían a algo similar a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  all     fw      tcp     25,465,587
ACCEPT  all     fw      tcp     110,143,993,995
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Al terminar de configurar las reglas para **Shorewall**, reinicie el muro cortafuegos, ejecutando el siguiente mandato:

```
service shorewall restart
```

61.5. Lecturas posteriores.

Se recomienda consultar los documentos titulados «**Cómo configurar Sendmail y Dovecot con soporte SSL/TLS**», «**Configuración avanzada de Sendmail**», «**Cómo instalar y configurar Spamassassin**» y «**Configuración simple para Antivirus y Antispam**».

62. Configuración de Sendmail y Dovecot con soporte SSL/TLS.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

62.1. Introducción.

Este documento requiere la lectura y comprensión previa del documento titulado «**Configuración básica de Sendmail**.»

62.1.1. Acerca de DSA.

DSA (**D**igital **S**ignature **A**lgorithm o Algoritmo de Firma digital) es un algoritmo creado por el NIST (**N**ational **I**nstitute of **S**tandards and **T**echnology o Instituto Nacional de Normas y Tecnología de EE.UU.), publicado el 30 de agosto de 1991, como propuesta para el proceso de firmas digitales. Se utiliza para firmar información, más no para cifrar ésta.

URL: http://es.wikipedia.org/wiki/DSA

62.1.2. Acerca de RSA.

RSA, acrónimo de los apellidos de sus autores, Ron **R**ivest, Adi **S**hamir y Len **A**dleman, es un algoritmo para el ciframeinto de claves públicas que fue publicado en 1977, patentado en EE.UU. en 1983 por el el Instituto Tecnológico de Michigan (**MIT**). **RSA** es utilizado ampliamente en todo el mundo para los protocolos destinados para el comercio electrónico.

URL: http://es.wikipedia.org/wiki/RSA

62.1.3. Acerca de X.509.

X.509 es un estándar **ITU-T** (estandarización de **T**elecomunicaciones de la **I**nternational **T**elecommunication **U**nion) para infraestructura de claves públicas (**PKI** o **P**ublic **K**ey **I**nfrastructure). Entre otras cosas, establece los estándares para certificados de claves públicas y un algoritmo para validación de ruta de certificación. Este último se encarga de verificar que la ruta de un certificado sea válida bajo una infraestructura de clave pública determinada. Es decir, desde el certificado inicial, pasando por certificados intermedios, hasta el certificado de confianza emitido por una Autoridad Certificadora (**CA** o **C**ertification **A**uthority).

URL: http://es.wikipedia.org/wiki/X.509

62.1.4. Acerca de OpenSSL.

OpenSSL es una implementación libre, de código abierto, de los protocolos **SSL** (**S**ecure **S**ockets **L**ayer o Nivel de Zócalo Seguro) y **TLS** (**T**ransport **L**ayer **S**ecurity o Seguridad para Nivel de Transporte). Está basado sobre el extinto proyecto **SSLeay**, iniciado por Eric Young y Tim Hudson, hasta que éstos comenzaron a trabajar para la división de seguridad de EMC Corporation.

URL: http://www.openssl.org/

62.2. Procedimientos.

Todos los procedimientos deben realizarse como el usuario **root**.

62.2.1. Generando firma digital y certificado para ambos servicios.

Acceda al directorio **/etc/pki/tls/**.

```
cd /etc/pki/tls/
```

La creación de la firma digital y certificado requiere utilizar una clave con algoritmo **RSA** de 2048 octetos (bits), con estructura **X.509** y sin DES. En el ejemplo a continuación, se establece una validez por 1825 días (cinco años) para el certificado creado:

```
openssl req -x509 -nodes -newkey rsa:2048 -days 1825 \
    -out certs/dominio.tld.crt -keyout private/dominio.tld.key
```

Lo anterior solicitará se ingresen varios datos:

- Código de dos letras para el país.
- Estado o provincia.
- Ciudad.
- Nombre de la empresa o razón social.
- Unidad o sección.
- Nombre del anfitrión.
- Dirección de correo.

La salida debe devolver algo similar a lo siguiente:

```
Generating a 1024 bit DSA private key
writing new private key to 'smtp.key'
-----
You are about to be asked to enter information that will be
incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name
or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:MX
State or Province Name (full name) [Berkshire]:Distrito Federal
Locality Name (eg, city) [Newbury]:Mexico
Organization Name (eg, company) [My Company Ltd]:Empresa, S.A. de C.V.
Organizational Unit Name (eg, section) []:Direccion Comercial
Common Name (eg, your name or your server's hostname) []:*.dominio.tld
Email Address []:webmaster@dominio.com
```

Si definió un nombre de anfitrión absoluto (ejemplo: mail.dominio.tld), el certificado sólo será válido cuando el servidor de correo electrónico sea invocado con el nombre definido en el campo **Common Name**. Es decir, sólo podrá utilizarlo cuando se defina **mail.dominio.tld** como servidor **SMTP**/**IMAP**/**POP3** con soporte **TLS** desde el cliente de correo electrónico. Funcionará incorrectamente si se invoca al servidor como, por mencionar un ejemplo, **correo.dominio.tld**. Es por eso que se sugiere utilizar ***.dominio.com** si se planea acceder hacia el mismo servidor con diferentes subdominios del mismo dominio.

A fin de facilitar a los clientes de correo electrónico el poder gestionar una futura actualización de certificado, conviene añadir una huella distintiva indubitable (fingerprint) al certificado.

```
openssl x509 -subject -fingerprint -noout -in certs/dominio.tld.crt
```

Es indispensable que todos los archivos de claves y certificados tengan permisos de acceso de sólo lectura para el usuario **root**:

```
chmod 400 certs/dominio.tld.crt private/dominio.tld.key
```

Regrese al directorio de inicio del usuario **root**.

```
cd
```

62.2.2. Configuración de Sendmail.

62.2.2.1. Parámetros de /etc/mail/sendmail.mc.

Edite el archivo /etc/mail/sendmail.mc:

```
vim /etc/mail/sendmail.mc
```

Es necesario configurar los siguiente parámetros a fin de que Sendmail utilice la clave y certificado recién creados:

```
define(`confCACERT_PATH',`/etc/pki/tls/certs')dnl
define(`confCACERT',`/etc/pki/tls/certs/ca-bundle.crt')dnl
define(`confSERVER_CERT',`/etc/pki/tls/certs/dominio.tld.crt')dnl
define(`confSERVER_KEY',`/etc/pki/tls/private/dominio.tld.key')dnl
```

El acceso cifrado con TLS es opcional si se realizan conexiones a través del puerto 25 y obligatorio si se hacen a través del puerto 465. El puerto 587 (submission), puede ser también utilizado para envío de correo electrónico. Por estándar se utiliza como puerto alternativo en los casos donde un cortafuegos impide a los usuarios acceder hacia servidores de correo trabajando por puerto 25. MS Outlook Express carece de soporte para usar TLS a través del puerto 587, pero el resto de los clientes de correo electrónico con soporte TLS si lo tienen.

A fin de habilitar el puerto 465 (smtps), a través de TCP, se debe descomentar la línea que contiene **DAEMON_OPTIONS(`Port=smtps, Name=TLSMTA, M=s')dnl**, como se muestra a continuación, resaltado en **negrita**:

```
dnl # The following causes sendmail to only listen on the IPv4 loopback address
dnl # 127.0.0.1 and not on any other network devices. Remove the loopback
dnl # address restriction to accept email from the internet or intranet.
dnl #
DAEMON_OPTIONS(`Port=smtp, Name=MTA')dnl
dnl #
dnl # The following causes sendmail to additionally listen to port 587 for
dnl # mail from MUAs that authenticate. Roaming users who can't reach their
dnl # preferred sendmail daemon due to port 25 being blocked or redirected find
dnl # this useful.
dnl #
DAEMON_OPTIONS(`Port=submission, Name=MSA, M=Ea')dnl
dnl #
dnl # The following causes sendmail to additionally listen to port 465, but
dnl # starting immediately in TLS mode upon connecting. Port 25 or 587 followed
dnl # by STARTTLS is preferred, but roaming clients using Outlook Express can't
dnl # do STARTTLS on ports other than 25. Mozilla Mail can ONLY use STARTTLS
dnl # and doesn't support the deprecated smtps; Evolution <1.1.1 uses smtps
dnl # when SSL is enabled-- STARTTLS support is available in version 1.1.1.
dnl #
dnl # For this to work your OpenSSL certificates must be configured.
dnl #
DAEMON_OPTIONS(`Port=smtps, Name=TLSMTA, M=s')dnl
dnl #
dnl # The following causes sendmail to additionally listen on the IPv6 loopback
dnl # device. Remove the loopback address restriction listen to the network.
```

A fin de que surtan efecto los cambios, es necesario reiniciar el servicio **sendmail**.

```
service sendmail restart
```

62.2.2.2. Comprobaciones.

Realice una conexión con el mandato **nc** (netcat) o bien el mandato **telnet**, al puerto 25 del sistema. Ingrese el mandato **EHLO** con el dominio configurado. La salida deberá devolver, entre todas las funciones del servidor y entre éstas debe devolver una línea que indica **STARTTLS**. La salida puede ser similar a la siguiente:

```
nc 127.0.0.1 25
220 dominio.com ESMTP Sendmail ; Sat, 19 Jun 2010 18:18:02 -0500
ehlo dominio.com
250-dominio.com Hello localhost.localdomain [127.0.0.1], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-AUTH LOGIN PLAIN
250-STARTTLS
250-DELIVERBY
250 HELP
QUIT
```

Para salir, sólo escriba QUIT y pulse la tecla ENTER.

Ejecute los siguientes mandatos para verificar el soporte SSL/TLS, estableciendo conexiones SSL y TLS hacia los puertos 25, 465 y 587:

```
openssl s_client -crlf -connect 127.0.0.1:25 -starttls smtp
openssl s_client -connect 127.0.0.1:465
openssl s_client -crlf -connect 127.0.0.1:587 -starttls smtp
```

La salida de todo lo anterior será muy extensa, mostrando la información de los certificados utilizados.

Al realizar la configuración del cliente de correo electrónico, podrá especificarse conexión por SSL, TLS o STARTTLS. Tras aceptar el certificado, deberá ser posible autenticar, con nombre de usuario y clave de acceso y enviar correo electrónico.

62.2.3. Configuración de Dovecot.

62.2.3.1. Configuración de Dovecot en CentOS 6 y Red Hat Enterprise Linux 6.

CentOS 6 y **Red Hat Enterprise Linux 6** utilizan la versión **2.0** de **Dovecot** y por lo cual cambia radicalmente la configuración respecto de la versión **1.0.x**, utilizada en **CentOS 5** y **Red Hat Enterprise Linux 5**.

Edite el archivo **/etc/dovecot/conf.d/10-ssl.conf**:

```
vim /etc/dovecot/conf.d/10-ssl.conf
```

Descomente las siguientes líneas resaltadas en negrita:

```
# SSL/TLS support: yes, no, required. <doc/wiki/SSL.txt>
ssl = yes

# PEM encoded X.509 SSL/TLS certificate and private key. They're opened before
# dropping root privileges, so keep the key file unreadable by anyone but
# root. Included doc/mkcert.sh can be used to easily generate self-signed
# certificate, just make sure to update the domains in dovecot-openssl.cnf
ssl_cert = </etc/pki/tls/certs/dominio.tld.crt
ssl_key = </etc/pki/tls/private/dominio.tld.key
```

A fin de que surtan efecto los cambios, es necesario reiniciar el servicio **dovecot**.

```
service dovecot restart
```

62.2.3.2. Configuración de Dovecot en CentOS 5 y Red Hat Enterprise Linux 5.

Edite el archivo **/etc/dominio.tld.conf**:

```
vim /etc/dominio.tld.conf
```

Asegúrese que el parámetro **protocols** estén establecidos como valores: **imap imaps pop3 pop3s**.

```
protocols = imap imaps pop3 pop3s
```

De modo predeterminado, el soporte SSL de **Dovecot** está activo. Verifique que el parámetro **ssl_disable** tenga el valor **no** o bien sólo esté comentado.

```
#ssl_disable = no
```

Y se especifican las rutas del certificado y clave a través de los parámetros **ssl_cert_file** y **ssl_key_file**, del siguiente modo:

```
ssl_cert_file = /etc/pki/tls/certs/dominio.tld.crt
ssl_key_file = /etc/pki/tls/private/dominio.tld.key
```

A fin de que surtan efecto los cambios, es necesario reiniciar el servicio **dovecot**.

```
service dovecot restart
```

62.2.4. Comprobaciones.

Ejecute los siguientes mandatos para verificar el soporte SSL/TLS, estableciendo conexiones SSL y TLS hacia los puertos 110, 995, 143 y 993:

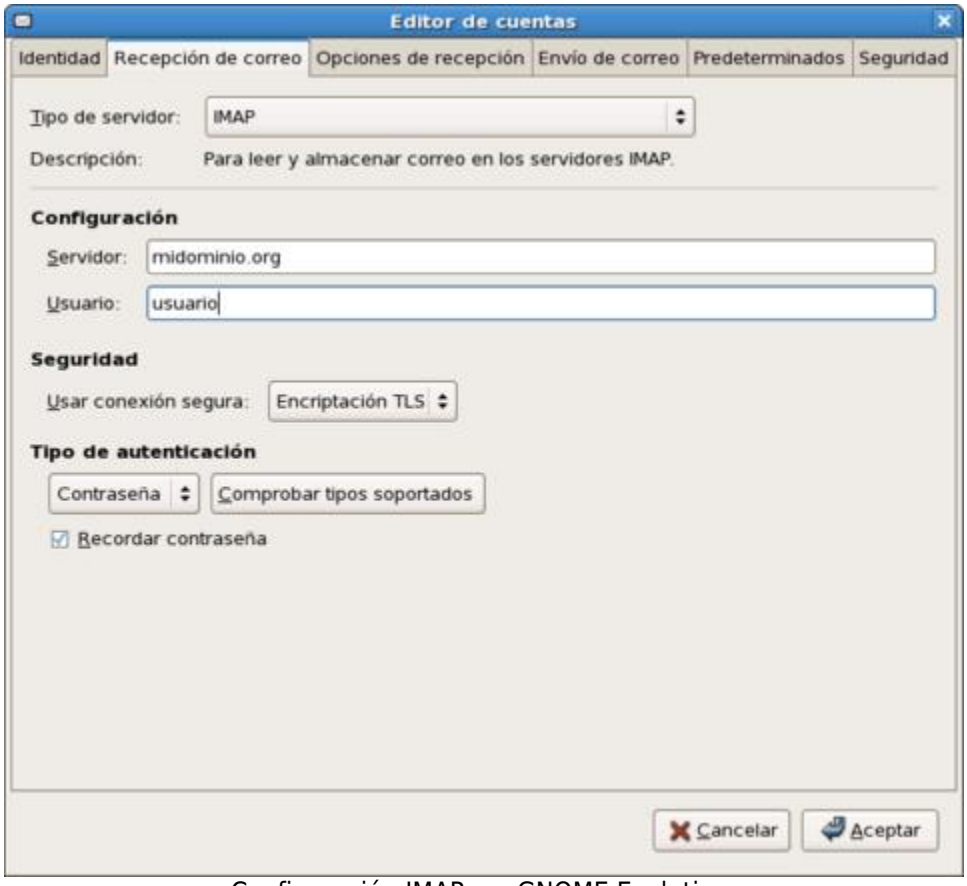
```
openssl s_client -connect 127.0.0.1:993
openssl s_client -connect 127.0.0.1:995
openssl s_client -crlf -connect 127.0.0.1:110 -starttls pop3
openssl s_client -crlf -connect 127.0.0.1:143 -starttls imap
```

La salida de todo lo anterior será muy extensa, mostrando la información de los certificados utilizados.

Si lo prefiere, utilice cualquier cliente de correo electrónico con soporte para SSL, TLS o STARTTLS y configure éste para conectarse hacia el sistema a través de **IMAPS** (puerto 993) o bien **POP3S** (puerto 995). Tras aceptar el certificado del servidor, el sistema deberá permitir autenticar, con nombre de usuario y clave de acceso y realizar la lectura del correo electrónico.

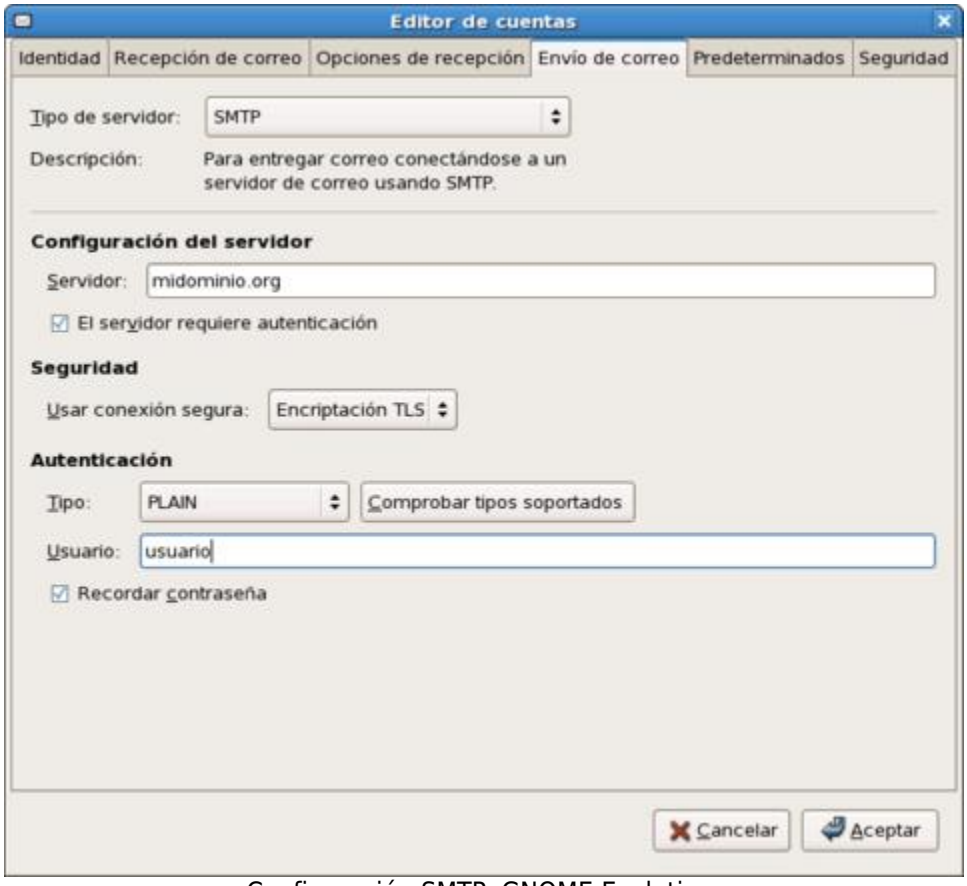
62.2.5. Configuración de GNOME Evolution.

Para GNOME Evolution, la configuración de IMAP o POP3 se realiza seleccionando el tipo de servidor, definiendo el nombre del servidor utilizado para crear el certificado, nombre de usuario y usar encriptación segura TLS.



Configuración IMAP, en GNOME Evolution.

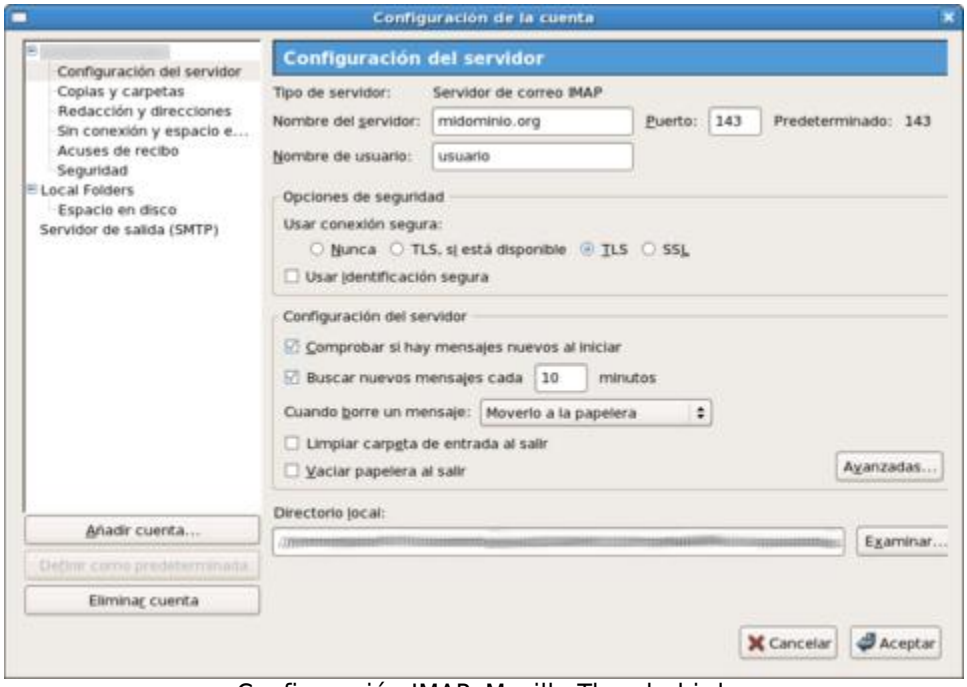
Se hace lo mismo para la configuración de SMTP (utilizar conexión segura TLS), pero considerando además que también se puede utilizar el puerto 587 (submission) en caso de que el proveedor de acceso a Internet del cliente haya restringido el uso del puerto 25 (smtp).



Configuración SMTP, GNOME Evolution.

62.2.6. Configuración Mozilla Thunderbird.

Para Mozilla Thunderbird, se define el nombre del servidor utilizado para crear el certificado, usuario y usar conexión segura TLS.



Configuración IMAP, Mozilla Thunderbird.

Se hace lo mismo para la configuración de SMTP (utilizar conexión segura TLS), pero considerando además que también se puede utilizar el puerto 587 (submission) en caso de que el proveedor de acceso a Internet del cliente haya restringido el uso del puerto 25 (smtp).

63. Configuración avanzada de Sendmail.

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

63.1. Antes de continuar.

Este documento requeire la lectura previa de los documentos titulados «**Introducción a los protocolos de correo electrónico**», «**Configuración básica de Sendmail**» y «**Cómo configurar Sendmail y Dovecot con soporte SSL/TLS**.»

63.2. Usuarios Virtuales.

Si se desea brindar un servicio de hospedaje de dominios virtuales, permitiendo que los usuarios envíen y reciban, correo electrónico, utilizando sus propios dominios, se deben **añadir** los siguientes parámetros **resaltados**, justo debajo de la función de **virtusertable** del archivo **/etc/mail/sendmail.mc**:

```
define(`confTO_IDENT', `0')dnl
dnl FEATURE(delay_checks)dnl
FEATURE(`no_default_msa', `dnl')dnl
FEATURE(`smrsh', `/usr/sbin/smrsh')dnl
FEATURE(`virtusertable',`hash -o /etc/mail/virtusertable.db')dnl
FEATURE(`genericstable',`hash -o /etc/mail/genericstable.db')dnl
GENERICS_DOMAIN_FILE(`/etc/mail/generics-domains')dnl
FEATURE(redirect)dnl
FEATURE(always_add_domain)dnl
FEATURE(use_cw_file)dnl
FEATURE(use_ct_file)dnl
```

Se generan tres archivos **nuevos** dentro del directorio `/etc/mail`:

```
touch /etc/mail/virtusertable
touch /etc/mail/genericstable
touch /etc/mail/generics-domains
```

El archivo **/etc/mail/virtusertable** sirve para definir qué cuentas virtuales de correo electrónico se entregan en ciertos buzones, de determinados usuarios. Edite el archivo **/etc/mail/virtusertable**:

```
vim /etc/mail/virtusertable
```

El formato de este archivo permite que **la separación de columnas se haga con tabuladores**, a fin de poder alinear los registros y poder tener todo mejor organizado. En el ejemplo a continuación, se entrega el correo de *webmaster@dominio1.net* en la cuenta mengano y el correo de *webmaster@dominio2.com*, en el buzón del usuario perengano:

```
webmaster@dominio1.net          mengano
webmaster@dominio2.com          perengano
```

Para hacer que el correo electrónico del usuario *mengano* salga del servidor como *webmaster@dominio1.net* y que el del usuario *perengano* salga como *webmaster@dominio2.com*, es necesario definir en el archivo **/etc/mail/genericstable**, el contenido contrario del archivo **/etc/mail/virtusertable**.

Genere el archivo **/etc/mail/genericstable**:

```
touch /etc/mail/genericstable
```

Edite el archivo **/etc/mail/genericstable**:

```
vim /etc/mail/generictable
```

Defina el contenido contrario del archivo en el archivo **/etc/mail/virtusertable**, del siguiente modo:

```
mengano                 webmaster@dominio1.net
perengano               webmaster@dominio2.com
```

Para efectos prácticos y **salvo que se requiera que haya más de una cuenta virtual de correo electrónico para un mismo usuario** o bien, **que dos o más usuarios emitan mensajes con la misma cuenta de correo electrónico**, se puede mantener sincronizados ambos archivos, trabajando directamente con **/etc/mail/virtusertable**, ejecutando el siguiente guión, el cual se encargará de pasar el texto desde el archivo **/etc/mail/virtusertable**, con el orden invertido de las columnas, hacia el archivo **/etc/mail/genericstable**.

```
while read cuenta usuario garbage
do
echo -e "${usuario}\t${cuenta}" >> /etc/mail/genericstable
done < /etc/mail/virtusertable
```

El archivo **/etc/mail/generics-domains** debe contener prácticamente lo mismo que el archivo **/etc/mail/local-host-names**, más los dominios que vayan a ser gestionados como dominios virtuales.

```
dominio.com
dominio1.net
dominio2.com
```

Invariablemente los archivos **/etc/mail/virtusertable.db** y **/etc/mail/genericstable.db**, deben actualizarse con el contenido de **/etc/mail/virtusertable** y **/etc/mail/genericstable**, respectivamente, cada vez que se se realicen cualquier tipo de cambio, como actualizar, añadir o eliminar, cuentas de correo virtuales.

```
for f in virtusertable genericstable
do
makemap hash /etc/mail/${f}.db < /etc/mail/${f}
done
```

63.3. Encaminamiento de dominios.

Sendmail incluye soporte para realizar en re-encaminamiento de dominios de correo a través del parámetro **FEATURE(`mailertable',`hash -o /etc/mail/mailertable.db')** que debe estar **habilitado de modo predeterminado** en el archivo **/etc/mail/sendmail.mc**. Esta función permite a Sendmail realizar traducción de dominios, especificar un agente de entrega y cambiar el encaminamiento establecido en un DNS.

63.3.1. Redundancia del servidor de correo.

Cuando se tiene un dominio de correo electrónico que recibe mucho tráfico, es conveniente establecer redundancia en el servicio para garantizar que el correo siempre será recibido y llegará a los buzones de correo hacia los que está destinado.

Se requieren dos servidores de correo. Uno deberá estar registrado en la zona del dominio en el DNS como **servidor de correo primario** (mail.dominio.com) y otro deberá estar registrado en la zona del dominio en el DNS como **servidor de correo secundario** (mail2.dominio.com) a fin de contar con redundancia.

1. Defina en la zona de DNS de dominio.com un servidor de correo primario (mail.dominio.com) y un servidor de correo secundario (mail2.dominio.com)
2. Configure normalmente el servidor de correo primario (mail.dominio.com) para administrar el correo de dominio.com.
3. Configure el servidor de correo secundario (mail2.dominio.com) del mismo modo, pero no añada dominio.com en el archivo **/etc/mail/local-host-names** ya que de otro modo el correo será tratado como local y jamas podrá ser entregado en el servidor de correo primario.
4. Debe de estar listado dominio.com en el archivo **/etc/mail/relay-domains** en el servidor de correo secundario (mail2.dominio.com) a fin de permitir la retransmisión de éste hacia el servidor de correo primario (mail.dominio.com).
5. En el servidor de correo secundario (mail2.dominio.com) modifique el archivo **/etc/mail/mailertable** y defina que dominio.com será entregado en el servidor de correo primario utilizando el nombre plenamente resuelto en la zona del DNS.

   ```
   dominio.com             smtp:mail.dominio.com
   ```

   Si lo desea, puede especificar la dirección IP en lugar del nombre:

   ```
   dominio.com             smtp:[172.16.1.50]
   ```

6. Reinicie Sendmail

   ```
   service sendmail restart
   ```

7. En adelante el correo de dominio.com será entregado normalmente y de primera instancia en el servidor de correo primario (mail.dominio.com), pero cuando éste, por alguna razón, se vea imposibilitado para recibir conexiones, el servidor de correo secundario (mail2.dominio.com) definido en la zona de DNS recibirá todo el correo de dominio.com y lo entregará en el servidor de correo primario (mail.dominio.com) cuando éste re-establezca operaciones normalmente.

63.3.2. Servidor de correo intermediario.

Sendmail puede servir de intermediario de correo electrónico ya sea para filtrado de correo con un antivirus, equipamiento lógico para filtrado de correo chatarra o bien como intermediario entre una red pública y un servidor en red local. Se requieren dos servidores de correo. Uno que será el servidor de correo intermediario (proxy.dominio.com), que de forma obligatoria deberá estar definido en la zona de DNS del dominio como servidor de correo primario (un registro MX) y otro que servirá como servidor de correo de destino (mail.dominio.com).

1. El servidor de correo que funcionará como intermediario (proxy.dominio.com) se configura normalmente, pero no añada dominio.com en el archivo **/etc/mail/local-host-names** ya que de otro modo el correo será tratado como local y jamas podrá ser entregado en el servidor de correo de destino (mail.dominio.com).
2. Debe de estar listado dominio.com en el archivo **/etc/mail/relay-domains** en el servidor de correo intermediario (proxy.dominio.com) a fin de permitir la retransmisión de éste hacia el servidor de correo primario (mail.dominio.com).
3. La dirección P del servidor de destino (mail.dominio.com) debe estar listada en el archivo **/etc/mail/access** con **RELAY** (retransmisión autorizada) del servidor de correo intermediario (proxy.dominio.com).
4. La dirección P del servidor de intermediario (proxy.dominio.com) debe estar listada en el archivo

/etc/mail/access con **RELAY** (retransmisión autorizada) del servidor de correo de destino (mail.dominio.com).

5. En el servidor de correo intermediario (proxy.dominio.com) modifique el archivo **/etc/mail/mailertable** y defina que dominio.com será entregado en el servidor de correo de destino (mail.dominio.com) utilizando el nombre **FQDN** (**F**ully **Q**ualified **D**omain **N**ame) y plenamente resuelto.

```
dominio.com             smtp:mail.dominio.com
```

6. Si lo desea, puede especificar la dirección IP en lugar del nombre:

```
dominio.com             smtp:[172.16.1.50]
```

7. En el servidor de correo de destino (mail.dominio.com), des-comente y defina **proxy.dominio.com** como valor para el parámetro **define(`SMART_HOST',`smtp.your.provider')**, de modo que **proxy.dominio.com** sea el servidor de retransmisión (smart host:

```
define(`SMART_HOST',`proxy.dominio.com')
```

8. Reinicie Sendmail en ambos servidores de correo.

```
service sendmail restart
```

63.4. Verificando el servicio.

Desde una terminal, ejecute el mandato **nc** dirigido hacia el puerto 25 de la dirección IP principal del sistema:

```
$ nc 192.168.0.254 25
```

Si Sendmail está funcionando correctamente, se establecerá una conexión exitosa y deberá devolver una salida similar a la siguiente:

```
Trying 172.16.1.50...
Connected to nombre.dominio (172.16.1.50).
Escape character is '^]'.
220 nombre.dominio ESMTP Sendmail 8.13.1/8.13.1; Sun, 5 Mar 2006 21:45:51 -0600
```

Ejecute el mandato **HELO** seguido del nombre del anfitrión:

```
HELO nombre.dominio
```

Obtendrá una salida similar a esta:

```
250 nombre.dominio Hello nombre.dominio [172.16.1.50], pleased to meet you
```

Ejecute el mandato **EHLO** seguido del nombre del anfitrión:

```
EHLO nombre.dominio
```

Obtendrá una salida similar a ésta y que mostrará las funciones del servidor:

```
250-nombre.dominio Hello nombre.dominio [172.16.1.50], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-AUTH DIGEST-MD5 CRAM-MD5
250-DELIVERBY
250 HELP
```

Ejecute el mandato **QUIT** para cerrar la conexión.

```
QUIT
```

El servidor deberá contestar lo siguiente al terminar la conexión:

```
221 2.0.0 nombre.dominio closing connection
Connection closed by foreign host.
```

La salida completa de todo el procedimiento anterior debe lucir similar a esto (mandatos utilizados resaltados en **negrita**):

```
[fulano@nombre ~]$ nc 172.16.1.50 25
Trying 172.16.1.50...
Connected to nombre.dominio (172.16.1.50).
Escape character is '^]'.
220 nombre.dominio ESMTP Sendmail 8.13.1/8.13.1; Sun, 5 Mar 2006 21:45:51 -0600
HELO nombre.dominio
250 nombre.dominio Hello nombre.dominio [172.16.1.50], pleased to meet you
EHLO nombre.dominio
250-nombre.dominio Hello nombre.dominio [172.16.1.50], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-AUTH DIGEST-MD5 CRAM-MD5
250-DELIVERBY
250 HELP
QUIT
221 2.0.0 nombre.dominio closing connection
Connection closed by foreign host.
```

63.5. Pruebas de envío de correo.

63.5.1. Utilizando nc.

Utilizar el mandato **nc** permite conocer y examinar como funciona realmente la interacción entre un servidor de correo y un cliente de correo.

Abra una sesión con **nc** dirigido hacia el puerto 25 de la dirección IP principal del sistema.

```
nc 172.16.1.50 25
```

Salude al sistema con el mandato **HELO** seguido del nombre del anfitrión.

```
HELO nombre.dominio
```

El servidor de correo deberá contestarle:

```
250 nombre.dominio Hello nombre.dominio [172.16.1.50], pleased to meet you
```

Ejecute el mandato **MAIL FROM** especificando la cuenta de correo de un usuario local de sus sistema del siguiente modo:

```
MAIL FROM: <fulano@nombre.dominio>
```

El servidor de correo deberá contestarle lo siguiente, a menos que especifique una cuenta de correo con un dominio distinto a los especificados en el archivo **/etc/mail/relay-domains**:

```
250 2.1.0 <fulano@nombre.dominio>... Sender ok
```

Ejecute el mandato **RCPT TO** especificando una cuenta de correo existente en el servidor del siguiente modo:

```
RCPT TO: <root@nombre.dominio>
```

El servidor de correo deberá contestarle lo siguiente:

```
250 2.1.5 <root@nombre.dominio>... Recipient ok
```

Ejecute el mandato **DATA**:

```
DATA
```

El servidor de correo deberá contestarle lo siguiente:

```
354 Enter mail, end with "." on a line by itself
```

Enseguida se ingresa el texto que desee incluir en le mensaje de correo electrónico. Al terminar finalice con un punto en una nueva línea.

```
Hola, este es un mensaje de prueba.
.
```

El sistema deberá contestarle algo similar a lo siguiente:

```
250 2.0.0 k263wEKK006209 Message accepted for delivery
```

Ejecute el mandato **QUIT**:

```
QUIT
```

El servidor deberá contestar lo siguiente al terminar la conexión:

```
221 2.0.0 nombre.dominio closing connection
Connection closed by foreign host.
```

La salida completa de todo el procedimiento anterior debe lucir similar a esto (mandatos utilizados resaltados en **negrita**):

```
[fulano@nombre ~]$ nc 172.16.1.50 25
Trying 172.16.1.50...
Connected to nombre.dominio (172.16.1.50).
Escape character is '^]'.
220 nombre.dominio ESMTP Sendmail 8.13.1/8.13.1; Sun, 5 Mar 2006 21:58:14
-0600
HELO nombre.dominio
250 nombre.dominio Hello nombre.dominio [172.16.1.50], pleased to meet you
MAIL FROM: <fulano@nombre.dominio>
250 2.1.0 <fulano@nombre.dominio>... Sender ok
RCPT TO: <root@nombre.dominio>
250 2.1.5 <root@nombre.dominio>... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
Hola, este es un mensaje de prueba.
.
250 2.0.0 k263wEKK006209 Message accepted for delivery
QUIT
221 2.0.0 nombre.dominio closing connection
Connection closed by foreign host.
```

63.5.2. Utilizando mutt.

Mutt, término utilizado en la lengua inglesa para referirse a perros mestizos, es un cliente de correo electrónico (MUA o **M**ail **U**ser **A**gent) para modo texto. Incluye soporte para color, hilos, MIME, PGP/GPG, protocolos POP3, IMAP y NNTP y para los formatos de correo **Maildir** y **mbox**.

Basta ejecutar mutt y pulsar las teclas indicadas la interfaz de texto para realizar diversas tareas. Para enviar un mensaje de correo electrónico siga este procedimiento:

1. Como usuario sin privilegios, ejecute **mutt**.
2. Responda con la tecla **«s»** para confirmar que se creará **~/Mail**.
3. Una vez iniciada la interfaz de texto de **mutt**, pulse la tecla **«m»** para crear un nuevo mensaje.
4. En la parte inferior de la pantalla aparece un diálogo para el destinatario (**To:**). Ingrese una cuenta de correo electrónico válida o alguna que exista al menos en el dominio de la Red Local (**LAN**).
5. En la parte inferior de la pantalla aparece un diálogo para ingresar el asunto del mensaje (**Subject:**). Ingrese un título para el mensaje.
6. Enseguida mutt iniciará **vi** para crear el texto que se enviará en el mensaje. Inicie el modo de **insertar** texto (**i**) de **vi** e ingrese algunas palabras. Al terminar, guarde y salga de **vi** (**:wq**).
7. Tras terminar con el editor de texto simple **vi**, **mutt** presentará una vista previa del mensaje. Confirme que los datos son los correctos y pulse la tecla **«y»** para enviar el mensaje. Si necesita cambiar alguno de éstos, pulse **«t»** para cambiar el destinatario o bien pulse la tecla **«s»**, para cambiar el campo de asunto del mensaje.
8. Mutt le devolverá a la pantalla principal. Si recibe un mensaje de respuesta, seleccione éste y pulse la tecla **ENTER** para visualizar el contenido.
9. Si desea responder el mensaje, pulse la tecla **«r»** y repita los procedimientos del paso 4 al 7.

Si lo desea, también puede utilizar mutt desde la linea de mandatos.

```
echo -e \
"Hola, soy ${USER} en ${HOSTNAME}.\n\
Por favor responde este mensaje.\n\nSaludos." \
| mutt \
-s "Mensaje enviado desde ${HOSTNAME}" \
fulano@maquina.dominio
```

Lo anterior envía un mensaje de correo electrónico hacia la cuenta fulano@maquina.dominio, con el asunto «**Mensaje enviado desde nombre.dominio**» con el siguiente contenido como texto del mensaje:

```
Hola, soy usuario en nombre.dominio
Por favor responde este mensaje.

Saludos.
```

64. Opciones avanzadas de seguridad para Sendmail.

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

64.1. Introducción.

Debido a la naturaleza del correo electrónico, es posible para un atacante inundar fácilmente el servidor y desencadenar en una denegación de servicio. Fenómenos como el denominado correo masivo no solicitado o Spam no hacen las cosas más fáciles y las administración de un servidor de correo puede tornarse una pesadilla. Añadir opciones avanzadas de seguridad se convierte en algo indispensable.

64.2. Funciones.

Todas las funciones explicadas a continuación pueden incluirse en el archivo `/etc/mail/sendmail.mc` justo debajo de la última línea que incluya `define` y arriba de la primera línea que incluya `FEATURE`.

64.2.1. confMAX_RCPTS_PER_MESSAGE

Este parámetro sirve para establecer un número máximo de destinatarios para un mensaje de correo electrónico. De modo predeterminado Sendmail establece un máximo de 256 destinatarios. En el siguiente ejemplo se limitará el número de destinatarios a 20:

```
define(`confMAX_RCPTS_PER_MESSAGE', `20')dnl
```

64.2.2. confBAD_RCPT_THROTTLE

Este parámetro sirve para establecer el tiempo de letargo que se utilizará por cada destinatario que sobrepase el límite establecido por `confMAX_RCPTS_PER_MESSAGE`. De modo predeterminado Sendmail no establece tiempo de letargo. En el siguiente ejemplo se establecerán 2 segundos de letargo por cada destinatario rechazado por sobrepasar el límite de destinatarios permitidos:

```
define(`confBAD_RCPT_THROTTLE', `2')dnl
```

64.2.3. confPRIVACY_FLAGS

Cuando se establece como valor `goaway', se deshabilitan varios mandatos SMTP como EXPN y VRFY, los cuales pudieran ser utilizados para revelar los nombres de usuarios locales a un spammer. También deshabilita las notificaciones de entrega, el cual es un mecanismo comunmente utilizado por quienes envían correo masivo no solicitado para verificar/confirmar la existencia de una cuenta activa y hace que el sistema solicite obligatoriamente HELO o EHLO antes de utilizar el mandato MAIL. Muchos programas de utilizados para enviar correo masivo no solicitado ni siquiera se molestan en utilizar HELO o EHLO. De modo predeterminado los valores de confPRIVACY_FLAGS son `authwarnings,novrfy,noexpn,restrictqrun', cambie por lo siguiente:

```
define(`confPRIVACY_FLAGS',`goaway')dnl
```

64.2.4. confMAX_HEADERS_LENGTH

Esté parámetro se utiliza para definir el tamaño máximo permitido para la cabecera de un mensaje en bytes. Algunos programas utilizados para enviar spam tratan de impedir que los MTA puedan registrar transacciones generando cabeceras muy grandes.

Limitar le tamaño de las cabeceras hace más difícil la ejecución de guión que explote vulnerabilidades recientes (desbordamientos de búfer) en UW IMAP, Outlook y Outlook Express.

La mayor parte de los mensajes de correo electrónico tendrán cabeceras de menos de 2 Kb (2048 bytes). Un mensaje de correo electrónico ordinario, por muy exagerado que resulte el tamaño de la cabecera, rara vez utilizará una cabecera que sobrepase los 5 Kb o 6 Kb, es decir, de 5120 o 6144 bytes. En el siguiente ejemplo se limitará el tamaño máximo de la cabecera de un mensaje a 16 Kb (requrerido para MailScanner):

```
define(`confMAX_HEADERS_LENGTH', `16384')dnl
```

El valor sugerido es 16 Kb (16384 bytes). Aumente o disminuya el valor a su discresión.

64.2.5. confMAX_MESSAGE_SIZE

Este parámetro sirve para especificar el tamaño máximo permitido para un mensaje de correo electrónico en bytes. Puede especificarse lo que el administrador considera apropiado. En el siguiente ejemplo se limitará el tamaño máximo de un mensaje a 3 MB:

```
define(`confMAX_MESSAGE_SIZE', `3145728')dnl
```

64.2.6. confMAX_DAEMON_CHILDREN

Este parámetro sirve para especificar cuantos procesos hijos se permitirán simultáneamente en el servidor de correo. De modo predeterminado sendmail no establece límites para este parámetro. Si se sobre pasa el límite de conexiones simultáneas, el resto serán demoradas hasta que se terminen las conexiones existentes y dejen lugar para nuevas conexiones. En el siguiente ejemplo se limitará el número de conexiones simultáneas hacia el servidor a 5:

```
define(`confMAX_DAEMON_CHILDREN', `5')dnl
```

64.2.7. confCONNECTION_RATE_THROTTLE

Este parámetro sirve para establecer el numero de conexiones máximas por segundo. De modo predeterminado sendmail no establece límites para este parámetro. En el siguiente ejemplo se limitará a 4 conexiones por segundo:

```
define(`confCONNECTION_RATE_THROTTLE', `4')dnl
```

65. Instalación y configuración de Postfix y Dovecot con soporte para TLS y autenticación.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales (incluyendo su publicación, a través de cualquier medio, por entidades con fines de lucro). c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en castellano. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

65.1. Introducción.

Es imprescindible primero estudiar y comprender, los conceptos descritos en el documento titulado «**Introducción a los protocolos de correo electrónico**.»

65.1.1. Acerca de Postfix.

Postfix, originalmente conocido por los nombres VMailer e IBM Secure Mailer, es un popular agente de transporte de correo (MTA o **M**ail **T**ransport **A**gent), creado con la principal intención de ser una alternativa más rápida, fácil de administrar y segura que Sendmail. Fue originalmente escrito por Wietse Venema durante su estancia en el Thomas J. Watson Research Center de IBM.

URL: http://www.postfix.org/.

65.1.2. Acerca de Dovecot.

Dovecot es un servidor de POP3 e IMAP de fuente abierta que funciona en Linux y sistemas basados sobre Unix™ y diseñado con la seguridad como principal objetivo. **Dovecot** puede utilizar tanto el formato **mbox** como **maildir** y es compatible con las implementaciones de los servidores UW-IMAP y Courier IMAP.

URL: http://dovecot.procontrol.fi/.

65.1.3. Acerca de SASL y Cyrus SASL.

SASL (**S**imple **A**uthentication and **S**ecurity **L**ayer) es un estructura para la seguridad de datos en protocolos de Internet. Desempareja mecanismos de la autenticación desde protocolos de aplicaciones, permitiendo, en teoría, cualquier mecanismo de autenticación soportado por SASL para ser utilizado en cualquier protocolo de aplicación que capaz de utilizar SASL. Actualmente SASL es un protocolo de la IETF (**I**nternet **E**ngineering **T**ask **F**orce) que ha sido propuesto como estándar. Está especificado en el **RFC 2222** creado por John Meyers en la Universidad Carnegie Mellon.

Cyrus SASL es una implementación de **SASL** que puede ser utilizada del lado del servidor o del lado del cliente y que incluye como principales mecanismos de autenticación soportados a ANONYMOUS, CRAM-MD5, DIGEST-MD5, GSSAPI y PLAIN. El código fuente incluye también soporte para los mecanismos LOGIN, SRP, NTLM, OPT y KERBEROS_V4.

URL: http://asg.web.cmu.edu/sasl/sasl-library.html.

65.1.4. Acerca de DSA.

DSA (**D**igital **S**ignature **A**lgorithm o Algoritmo de Firma digital) es un algoritmo creado por el NIST (**N**ational **I**nstitute of **S**tandards and **T**echnology o Instituto Nacional de Normas y Tecnología de EE.UU.), publicado el 30 de agosto de 1991, como propuesta para el proceso de firmas digitales. Se utiliza para firmar información, más no para cifrar ésta.

URL: http://es.wikipedia.org/wiki/DSA

65.1.5. Acerca de RSA.

RSA, acrónimo de los apellidos de sus autores, Ron **R**ivest, Adi **S**hamir y Len **A**dleman, es un algoritmo para el ciframiento de claves públicas que fue publicado en 1977, patentado en EE.UU. en 1983 por el el Instituto Tecnológico de Michigan (**MIT**). **RSA** es utilizado ampliamente en todo el mundo para los protocolos destinados para el comercio electrónico.

URL: http://es.wikipedia.org/wiki/RSA

65.1.6. Acerca de X.509.

X.509 es un estándar **ITU-T** (estandarización de **T**elecomunicaciones de la **I**nternational **T**elecommunication **U**nion) para infraestructura de claves públicas (**PKI** o **P**ublic **K**ey **I**nfrastructure). Entre otras cosas, establece los estándares para certificados de claves públicas y un algoritmo para validación de ruta de certificación. Este último se encarga de verificar que la ruta de un certificado sea válida bajo una infraestructura de clave pública determinada. Es decir, desde el certificado inicial, pasando por certificados intermedios, hasta el certificado de confianza emitido por una Autoridad Certificadora (**CA** o **C**ertification **A**uthority).

URL: http://es.wikipedia.org/wiki/X.509

65.1.7. Acerca de OpenSSL.

OpenSSL es una implementación libre, de código abierto, de los protocolos **SSL** (**S**ecure **S**ockets **L**ayer o Nivel de Zócalo Seguro) y **TLS** (**T**ransport **L**ayer **S**ecurity o Seguridad para Nivel de Transporte). Está basado sobre el extinto proyecto **SSLeay**, iniciado por Eric Young y Tim Hudson, hasta que éstos comenzaron a trabajar para la división de seguridad de EMC Corporation.

URL: http://www.openssl.org/

65.2. Equipamiento lógico necesario.

Instalar los paquetes **postfix**, **dovecot**, **cyrus-sasl** y **cyrus-sasl-plain**:

```
yum -y install postfix dovecot cyrus-sasl cyrus-sasl-plain
```

Si acaso estuviese instalado, elimine el paquete cyrus-sasl-gssapi, ya que este utiliza el método de autenticación GSSAPI, mismo que requeriría de la base de datos de cuentas de usuario de un servidor Kerberos:

```
yum remove cyrus-sasl-gssapi
```

De igual manera, si estuviese instalado, elimine el paquete cyrus-sasl-md5, ya que este utiliza los métodos de autenticación CRAM-MD5 y Digest-MD5, mismos que requerían asignar las claves de acceso para SMTP a través del mandato saslpasswd2. Outlook carece de soporte para estos métodos de autenticación.

```
yum remove cyrus-sasl-md5
```

65.3. Procedimientos.

Todos los procedimientos deben realizarse como el usuario **root**.

65.3.1. Definiendo Postfix como agente de transporte de correo predeterminado.

El mandato **alternatives**, con la opción **alternatives**--config mta, se utiliza para conmutar el servicio de correo electrónico del sistema y elegir que paquete utilizar. Sólo es necesario utilizar éste si previamente estaban instalados Sendmail o Exim. Sí este es el caso, ejecute lo siguiente desde una terminal y defina **Postfix** como agente de transporte de correo (**MTA**, **M**ail **T**ransport **A**gent), seleccionado éste.

```
alternatives --config mta
```

Lo anterior devolverá una salida similar a la siguiente, donde deberá elegir entre **postfix** y **sendmail** como MTA predeterminado del sistema:

```

Hay 2 programas que proporcionan 'mta'.

  Selección    Comando
-----------------------------------------------
*+ 1           /usr/sbin/sendmail.postfix
   2           /usr/sbin/sendmail.sendmail

Presione Intro para mantener la selección actual[+] o escriba el número de la selección:  1
```

Si estuviera presente **sendmail**, detenga éste (es el **MTA** predeterminado en **CentOS 5** y **Red Hat Enterprise Linux 5**) e inicie postfix:

```
service sendmail stop
chkconfig sendmail off
service postfix start
chkconfig postfix on
```

65.3.2. SELinux y Postfix.

A fin de que SELinux permita a Postfix escribir el el directorio de entrada de correo electrónico (**/var/spool/mail/**), es necesario habilitar la siguiente política:

```
setsebool -P allow_postfix_local_write_mail_spool 1
```

Solo en **CentOS 5** y **Red Hat Enterpise Linux 5**, a fin de que SELinux permita la lectura de correo electrónico, es necesario habilitar la siguiente política:

```
setsebool -P mail_read_content 1
```

En **CentOS 6** y **Red Hat Enterpise Linux 6**, esta política dejó de existir, pues se volvió innecesaria.

65.3.3. Configuración de Postfix.

65.3.4. Generando firma digital y certificado para ambos servicios.

Acceda al directorio **/etc/pki/tls/**.

```
cd /etc/pki/tls/
```

La creación de la firma digital y certificado requiere utilizar una clave con algoritmo **RSA** de 2048 octetos (bits), con estructura **X.509** y sin DES. En el ejemplo a continuación, se establece una validez por 1825 días (cinco años) para el certificado creado:

```
openssl req -x509 -nodes -newkey rsa:2048 -days 1825 \
    -out certs/dominio.tld.crt -keyout private/dominio.tld.key
```

Lo anterior solicitará se ingresen varios datos:

- Código de dos letras para el país.
- Estado o provincia.
- Ciudad.
- Nombre de la empresa o razón social.
- Unidad o sección.
- Nombre del anfitrión.
- Dirección de correo.

La salida debe devolver algo similar a lo siguiente:

```
Generating a 1024 bit DSA private key
writing new private key to 'smtp.key'
-----
You are about to be asked to enter information that will be
incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name
or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:MX
State or Province Name (full name) [Berkshire]:Distrito Federal
Locality Name (eg, city) [Newbury]:Mexico
Organization Name (eg, company) [My Company Ltd]:Empresa, S.A. de C.V.
Organizational Unit Name (eg, section) []:Direccion Comercial
Common Name (eg, your name or your server's hostname) []:*.dominio.tld
Email Address []:webmaster@dominio.com
```

Si definió un nombre de anfitrión absoluto (ejemplo: mail.dominio.tld), el certificado sólo será válido cuando el servidor de correo electrónico sea invocado con el nombre definido en el campo **Common Name**. Es decir, sólo podrá utilizarlo cuando se defina **mail.dominio.tld** como servidor **SMTP**/**IMAP**/**POP3** con soporte **TLS** desde el cliente de correo electrónico. Funcionará incorrectamente si se invoca al servidor como, por mencionar un ejemplo, **correo.dominio.tld**. Es por eso que se sugiere utilizar ***.dominio.com** si se planea acceder hacia el mismo servidor con diferentes subdominios del mismo dominio.

A fin de facilitar a los clientes de correo electrónico el poder gestionar una futura actualización de certificado, conviene añadir una huella distintiva indubitable (fingerprint) al certificado.

```
openssl x509 -subject -fingerprint -noout -in certs/dominio.tld.crt
```

Es indispensable que todos los archivos de claves y certificados tengan permisos de acceso de sólo lectura para el usuario **root**:

```
chmod 400 certs/dominio.tld.crt private/dominio.tld.key
```

Regrese al directorio de inicio del usuario **root**.

```
cd
```

65.3.4.1. Archivo de configuración /etc/postfix/master.cf.

Editar el archivo **/etc/postfix/master.cf**:

```
vim /etc/postfix/master.cf
```

Si utiliza **CentOS 5** o **Red Hat Enterprise Linux 5**, debe descomentar las siguientes líneas resaltadas en **negrita**:

```
smtp      inet  n       -       n       -       -       smtpd
submission inet n       -       n       -       -       smtpd
  -o smtpd_enforce_tls=yes
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
smtps     inet  n       -       n       -       -       smtpd
  -o smtpd_tls_wrappermode=yes
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
```

Si utiliza **CentOS 6** o **Red Hat Enterprise Linux 6**, debe descomentar las siguientes líneas resaltadas en **negrita**:

```
smtp      inet  n       -       n       -       -       smtpd
submission inet n       -       n       -       -       smtpd
  -o smtpd_tls_security_level=encrypt
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
  -o milter_macro_daemon_name=ORIGINATING
smtps     inet  n       -       n       -       -       smtpd
  -o smtpd_tls_wrappermode=yes
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
  -o milter_macro_daemon_name=ORIGINATING
```

65.3.4.2. Archivo de configuración /etc/postfix/main.cf.

A continuación, se debe editar el archivo **/etc/postfix/main.cf**:

```
vim /etc/postfix/main.cf
```

Respetando el resto del contenido original de este archivo y asumiendo que el nombre de anfitrión del servidor es **mail.dominio.com** y que se va a utilizar para gestionar el correo electrónico de **dominio.com**, solo se deben **localizar y configurar** los siguientes parámetros:

```
# Todo lo siguiente solo requiere descomentarse o bien modificar la línea
# correspondiente que esté descomentada.

# Definir el nombre de anfitrión del sistema (hostname).
myhostname = mail.dominio.com

# Definir el dominio principal a gestionar.
mydomain = dominio.com

myorigin = $mydomain

# Definir se trabaje por todas las interfaces.
# De modo predeterminado solo trabaja por la interfaz de retorno del sistema
# (loopback), es decir, solo escucha peticiones a través de sobre 127.0.0.1
#inet_interfaces = localhost
inet_interfaces = all

# Si se van a manejar más dominios de correo electrónico, añadirlos también.
mydestination = $myhostname, $mydomain, localhost.localdomain, localhost

# Definir tus redes locales, ejemplo asume que tu LAN es 192.168.1.0/24
mynetworks = 192.168.1.0/24, 127.0.0.0/8

# Si se van a manejar más dominios de correo electrónico, añadirlos también.
relay_domains = $mydestination

# Importante para poder utilizar procmail para filtrar correo.
mailbox_command = /usr/bin/procmail

# Todo lo siguiente está ausente en la configuración.
# Añadir todo al final del archivo main.cf
#
smtpd_tls_security_level = may
smtpd_tls_CAfile = /etc/pki/tls/certs/ca-bundle.crt
# Las rutas deben corresponder a las del certificado y firma digital creados.
smtpd_tls_key_file = /etc/pki/tls/private/dominio.tld.key
smtpd_tls_cert_file = /etc/pki/tls/certs/dominio.tld.crt
smtpd_tls_auth_only = no
smtp_use_tls = yes
smtpd_use_tls = yes
smtp_tls_note_starttls_offer = yes
smtpd_tls_loglevel = 1
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s
tls_random_source = dev:/dev/urandom


# Soporte para autenticar a través de SASL.
# smtpd_sasl_local_domain = # Solo como referencia.
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_sasl_authenticated_header = yes
smtpd_recipient_restrictions = permit_sasl_authenticated,permit_mynetworks,reject_unauth_destination
```

A fin de ahorrar tiempo realizando búsqueda de los parámetros anteriores, todo lo anterior también se puede configurar utilizando el mandato **postconf**, del siguiente modo:

```
postconf -e 'myhostname = mail.dominio.com'
postconf -e 'mydomain = dominio.com'
postconf -e 'myorigin = $mydomain'
postconf -e 'inet_interfaces = all'
postconf -e 'mydestination = $myhostname, $mydomain, localhost.localdomain, localhost'
postconf -e 'mynetworks = 192.168.1.0/24, 127.0.0.0/8'
postconf -e 'relay_domains = $mydestination'
postconf -e 'mailbox_command = /usr/bin/procmail'
postconf -e 'smtpd_tls_CAfile = /etc/pki/tls/certs/ca-bundle.crt'
postconf -e 'smtpd_tls_key_file = /etc/pki/tls/private/dominio.tld.key'
postconf -e 'smtpd_tls_cert_file = /etc/pki/tls/certs/dominio.tld.crt'
postconf -e 'smtpd_tls_auth_only = no'
postconf -e 'smtp_use_tls = yes'
postconf -e 'smtpd_use_tls = yes'
postconf -e 'smtp_tls_note_starttls_offer = yes'
postconf -e 'smtpd_tls_loglevel = 1'
postconf -e 'smtpd_tls_received_header = yes'
postconf -e 'smtpd_tls_session_cache_timeout = 3600s'
postconf -e 'tls_random_source = dev:/dev/urandom'
postconf -e 'smtpd_sasl_auth_enable = yes'
postconf -e 'smtpd_sasl_security_options = noanonymous'
postconf -e 'broken_sasl_auth_clients = yes'
postconf -e 'smtpd_sasl_authenticated_header = yes'
postconf -e 'smtpd_recipient_restrictions =
permit_sasl_authenticated,permit_mynetworks,reject_unauth_destination'
```

65.3.4.3. Archivo de configuración /etc/aliases.

Se debe editar también el archivo **/etc/aliases**:

```
vim /etc/aliases
```

Se debe definir que el correo del usuario **root** se entregue al cualquier otro usuario del sistema. El objetivo de esto es que jamás se tenga necesidad de utilizar la cuenta del usuario **root** y se prefiera en su lugar una cuenta de usuario sin privilegios. Solo se requiere descomentar la última línea de este archivo, que como ejemplo entrega el correo del usuario **root** al usuario **marc** y definir un usuario existente en el sistema

```
#root:  marc
root:   fulano
```

Al terminar, se ejecuta el mandato **postalias** para generar el archivo **/etc/aliases.db** que será utilizado por **Postfix**:

```
postalias /etc/aliases
```

65.3.5. Configuración de Dovecot en CentOS 5 y Red Hat Enterprise Linux 5.

65.3.5.1. Parámetros del archivo /etc/dovecot.conf.

Editar el archivo **/etc/dovecot.conf**:

```
vim /etc/dovecot.conf
```

En el parámetro **protocols**, se deben activar todos los servicios (imap, imaps, pop3 y pop3s).

```
protocols = imap imaps pop3 pop3s
```

De modo predeterminado, el soporte SSL de **Dovecot** está activo. Verifique que el parámetro **ssl_disable** tenga el valor **no** o bien solo esté comentado.

```
#ssl_disable = no
```

Y se especifican las rutas del certificado y clave a través de los parámetros **ssl_cert_file** y **ssl_key_file**, del siguiente modo:

```
ssl_cert_file = /etc/pki/tls/certs/dominio.tld.crt
ssl_key_file = /etc/pki/tls/private/dominio.tld.key
```

65.3.6. Configuración de Dovecot en CentOS 6 y Red Hat Enterprise Linux 6.

CentOS 6 y **Red Hat Enterprise Linux 6** utilizan la versión **2.0** de **Dovecot** y por lo cual cambia radicalmente la configuración respecto de la versión **1.0.x**, utilizada en **CentOS 5** y **Red Hat Enterprise Linux 5**.

65.3.6.1. Parámetros del archivo /etc/dovecot/dovecot.conf.

Edite el archivo **/etc/dovecot/dovecot.conf** y descomente el parámetro **protocolos**, estableciendo como valor **pop3 imap lmtp**.

```
# Protocols we want to be serving.
protocols = imap pop3
```

65.3.6.2. Parámetros del archivo /etc/dovecot/conf.d/10-mail.conf.

Alrededor de la línea 30 del archivo **/etc/dovecot/conf.d/10-mail.conf**, establezca **mbox:~/mail:INBOX=/var/mail/%u** como valor del parámetro **mail_location**.

```
mail_location = mbox:~/mail:INBOX=/var/mail/%u
```

65.3.6.3. Parámetros del archivo /etc/dovecot/conf.d/10-ssl.conf.

En el archivo **/etc/dovecot/conf.d/10-ssl.conf**, descomente las siguientes líneas resaltadas en negrita:

```
# SSL/TLS support: yes, no, required. <doc/wiki/SSL.txt>
ssl = yes

# PEM encoded X.509 SSL/TLS certificate and private key. They're opened before
# dropping root privileges, so keep the key file unreadable by anyone but
# root. Included doc/mkcert.sh can be used to easily generate self-signed
# certificate, just make sure to update the domains in dovecot-openssl.cnf
ssl_cert = </etc/pki/tld/certs/dominio.tld.key
ssl_key = </etc/pki/tls/private/dominio.tld.key
```

65.3.7. Iniciar servicios y añadir éstos al arranque del sistema.

Se deben añadir al arranque del sistema e iniciar (o reiniciar) los servicios **saslauthd**, **dovecot** y **postfix**:

```
chkconfig saslauthd on
chkconfig dovecot on
chkconfig postfix on
service saslauthd start
service dovecot start
service postfix restart
```

65.3.8. Soporte para LMTP.

Si utiliza **CentOS 6** o **Red hat Enterprise Linux 6**, es decir **Dovecot 2.0** y **Postfix 2.6.6**, podrá utilizar **LMTP** (**L**ocal **M**ail **T**ransfer **P**rotocol) o protocolo de transporte local de correo. Este protocolo esta basado sobre el protocolo SMTP y está diseñado como una alternativa a SMTP para situaciones donde el lado receptor carece de cola de correo (*queue mail*), como un MTA que entiende conversaciones SMTP. Puede ser utilizado como una forma alternativa y más eficiente para el transporte de correo entre Postfix y Dovecot.

Edite el archivo **/etc/dovecot/dovecot.conf** y añada **lmtp** a los valores del parámetro **protocolos**, de la siguiente forma.

```
# Protocols we want to be serving.
protocols = imap pop3 lmtp
```

A fin de poder hacer uso de **LMTP** de manera apropiada, es necesario añadir el siguiente parámetro en el archivo **/etc/postfix/main.cf**:

```
virtual_transport = lmtp:unix:/var/run/dovecot/lmtp
```

O bien ejecutar lo siguiente:

```
postconf -e 'virtual_transport = lmtp:unix:/var/run/dovecot/lmtp'
```

Y reiniciar los servicios **dovecot** y **postfix**.

```
service dovecot restart
service postfix restart
```

65.3.9. Modificaciones necesarias en el muro cortafuegos.

Si se utiliza un cortafuegos con políticas estrictas, como por ejemplo **Shorewall**, es necesario abrir, además de los puertos 25, 110, 143 y 587 por TCP (**SMTP**, **POP3**, **IMAP** y **Submission**, respectivamente), los puertos 465, 993 y 995 por TCP (**SMTPS**, **IMAP** y **POP3S**, respectivamente).

Editar el archivo **/etc/shorewall/rules**:

```
vim /etc/shorewall/rules
```

Las reglas para el archivo **/etc/shorewall/rules** de **Shorewall** correspondería a algo similar a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  net     fw      tcp     25,110,143,465,587,993,995
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Para que tomen efecto los cambios, hay que reiniciar el servicio Shorewall.

```
service shorewall restart
```

65.3.10. Requisitos en la zona de reenvío en el servidor DNS.

Es indispensable que exista un DNS que resuelva correctamente el dominio y apunte el servicio de correo electrónico hacia la IP del servidor de correo electrónico recién configurado. Asumiendo que se hizo correctamente todo lo mencionado en este documento, la única forma en que se imposibilitaría la llegada y/o salida del correo electrónico se esté utilizando un enlace ADSL con IP dinámica (restringido por le proveedor para utilizar el puerto 25) o bien que el servidor DNS que resuelve el dominio, esté apuntando hacia otra dirección IP para el servicio de correo electrónico. En el DNS se requieren al menos los siguientes registros, donde **xx.xx.xx.xx** corresponde a la IP del servidor de correo electrónico.

```
$TTL 86400
@       IN      SOA     dns1.isp.com    alguien.algo.com (
                2010061901 ; Número de serie
                28800 ; Tiempo de refresco
                7200 ; Tiempo entre reintentos
                604800 ; tiempo de espiración
                86400 ; Tiempo total de vida
                )
@       IN              NS      dns1.isp.com.
@       IN              NS      dns2.isp.com.
@       IN              A       a.b.c.d
@       IN              MX      10      mail
@       IN              TXT     "v=spf1 a mx -all"
mail    IN              A       xx.xx.xx.xx
www     IN              A       a.b.c.d
ftp     IN              A       a.b.c.d
```

65.4. Comprobaciones.

65.4.1. A través de terminal.

Realice una conexión con el mandato **nc** (netcat) o bien el mandato **telnet**, al puerto 25 del sistema. Ingrese el mandato **EHLO** con el dominio configurado. La salida deberá devolver, entre todas las funciones del servidor, una línea que indica **STARTTLS**. La salida puede ser similar a la siguiente:

```
nc 127.0.0.1 25
220 emachine.alcancelibre.org ESMTP Postfix
EHLO dominio.com
250-mail.dominio.com
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH PLAIN LOGIN
250-AUTH=PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
QUIT
```

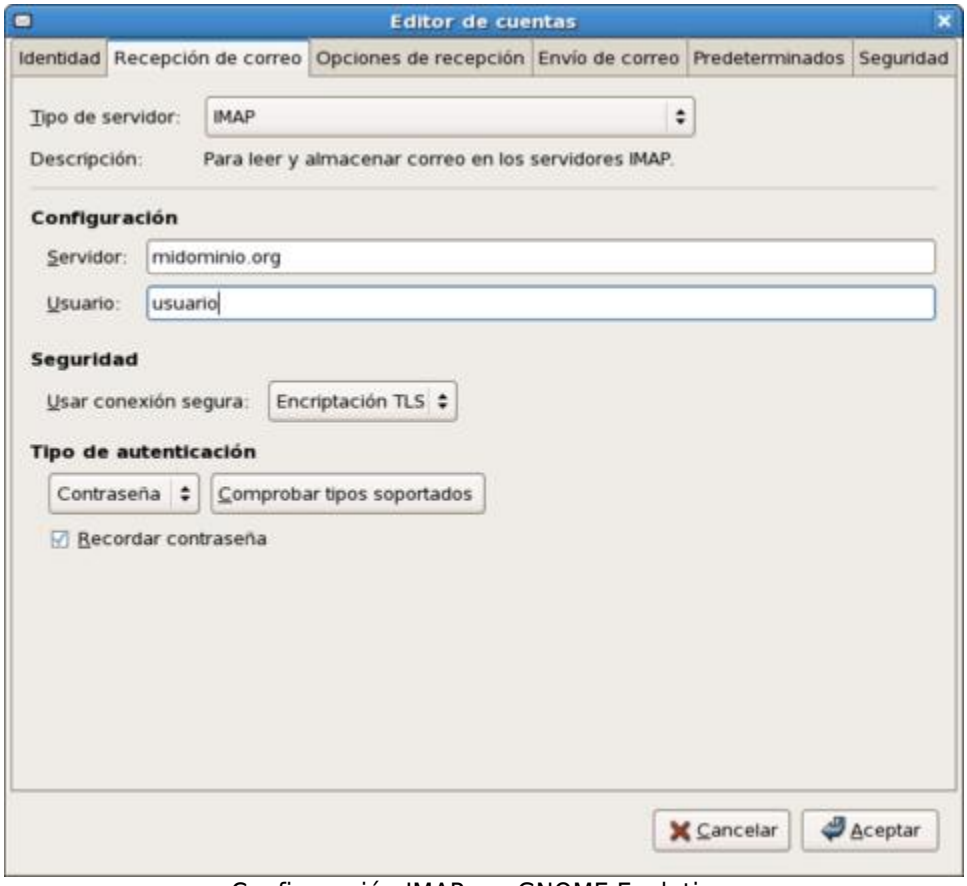
Para salir, solo escriba QUIT y pulse la tecla ENTER.

65.4.2. A través de clientes de correo electrónico.

Utilice cualquier cliente de correo electrónico con soporte para TLS/SSL y configure éste para conectarse hacia el sistema a través de **IMAPS** (puerto 993) o bien **POP3S** (puerto 995). Tras aceptar el certificado del servidor, el sistema deberá permitir autenticar, con nombre de usuario y clave de acceso y realizar la lectura del correo electrónico.

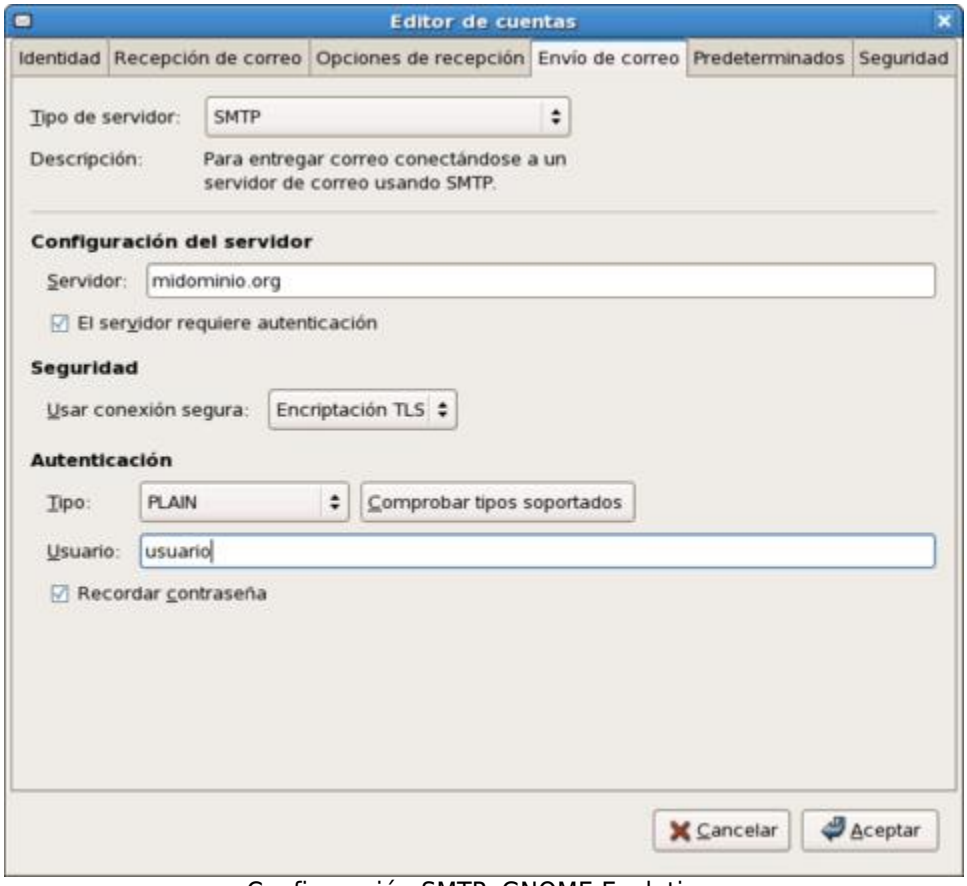
65.4.2.1. Configuración de GNOME Evolution.

Para GNOME Evolution, la configuración de IMAP o POP3, se realiza seleccionando el tipo de servidor, definiendo el nombre del servidor utilizado para crear el certificado, nombre de usuario y usar encriptación segura TLS.



Configuración IMAP, en GNOME Evolution.

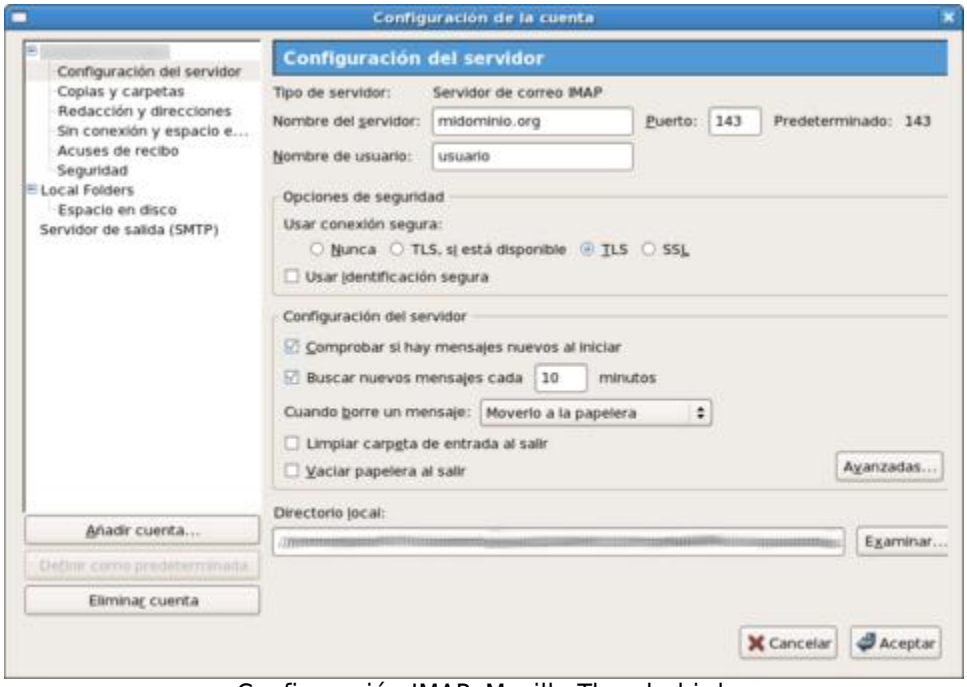
Se hace lo mismo para la configuración de SMTP (utilizar conexión segura TLS), pero considerando además que también se puede utilizar el puerto 587 (submission) en caso de que el proveedor de acceso a Internet del cliente haya restringido el uso del puerto 25 (smtp).



Configuración SMTP, GNOME Evolution.

65.4.2.2. Configuración Mozilla Thunderbird.

Para Mozilla Thunderbird, se define el nombre del servidor utilizado para crear el certificado, usuario y usar conexión segura TLS.



Configuración IMAP, Mozilla Thunderbird.

Se hace lo mismo para la configuración de SMTP (utilizar conexión segura TLS), pero considerando además que también se puede utilizar el puerto 587 (submission) en caso de que el proveedor de acceso a Internet del cliente haya restringido el uso del puerto 25 (smtp).

Configuración SMTP, Mozilla Thunderbird.

65.5. Modificaciones necesarias en el muro cortafuegos.

Si se utiliza un cortafuegos con políticas estrictas, como por ejemplo **Shorewall**, es necesario abrir, además de los puertos 25, 110, 143 y 587 por TCP (**SMTP**, **POP3**, **IMAP** y **Submission**, respectivamente), los puertos 465, 993 y 995 por TCP (**SMTPS**, **IMAP** y **POP3S**, respectivamente).

La regla para el archivo **/etc/shorewall/rules** de **Shorewall** correspondería a algo similar a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  all     fw      tcp     25,110,143,465,587,993,995
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

66. Cómo instalar y configurar Amavisd-new con Postfix en CentOS.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales (incluyendo su publicación, a través de cualquier medio, por entidades con fines de lucro). c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en castellano. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

66.1. Introducción.

Este documento permitirá configurar Postfix para utilizar amavisd-new para el control de virus y correo *spam*. Se requiere haber configurado previamente Postfix de la forma en que se describe en el documento titulado «*Cómo instalar y configurar Postfix en CentOS 5 con soporte para TLS y autenticación*.»

66.1.1. Acerca de Amavisd-new.

Amavisd-new es una interfaz confiable y de alto desempeño entre el agente de trasporte de correo (**MTA**, **M**ail **T**ransport **A**gent) y uno o más supervisores de contenido, como es el caso de supervisores anti-virus, y/o SpamAssassin. Está escrito en Perl para asegurar su alta confiabilidad, portabilidad y facilidad de mantenimiento.

Funciona comunicándose con el MTA a través de **ESMTP** (**E**xtended Simple **M**ail **T**ransfer **P**rotocol o Protocolo Simple de Transferencia de Correo) o bien **LMTP** (**L**ocal **M**ail **T**ransfer **P**rotocol o Protocolo de Transferencia Local de Correo), a través de programas auxiliares, con un diseño que impide se puede parder correo electrónico de manera incidental.

URL: http://www.ijs.si/software/amavisd/

66.2. Equipamiento lógico necesario.

66.2.1. Creación del usuario para ClamAV.

De modo predeterminado, en los paquetes RPM basados sobre los disponibles para Fedora, el usuario para ClamAV se asigna a través de los mandatos **fedora-groupadd** y **fedora-useradd** el UID y GID 4 en el sistema. A fin de prevenir un conflicto de UID/GID con otros usuarios y grupos de sistema, se recomienda crear previamente al grupo y usuario correspondientes para ClamAV:

```
groupadd -r clamav
useradd -r -s /sbin/nologin -d /var/lib/clamav -M -c 'Clamav Antivirus' -g clamav
clamav
```

66.2.2. Configuración de depósitos YUM para CentOS 5 y Red Hat Enterprise Linux 5.

Se pueden utilizar el siguiente depósito YUM para la plataforma Enterprise Linux 5.

```
[AL-Server]
name=Enterprise Linux $releasever - $basearch - AL Server
mirrorlist=http://www.alcancelibre.org/al/el$releasever/al-server
gpgkey=http://www.alcancelibre.org/al/AL-RPM-KEY
```

Instalar los paquetes necesarios se utiliza el siguiente mandato:

```
yum -y install amavisd-new clamav-update clamav-server cabextract tnef
yum -y install arj lha unzoo p7zip p7zip-plugins
```

Lo anterior también instalará todas las dependencias necesarias.

66.3. Procedimientos.

66.3.1. Configuración de SELinux.

66.3.1.1. Procedimiento para crear política.

Crear el directorio /**usr/share/selinux/packages/amavisd**:

```
mkdir /usr/share/selinux/packages/amavisd
```

Cambiarse al directorio /**usr/share/selinux/packages/amavisd**:

```
cd /usr/share/selinux/packages/amavisd
```

Descargar desde **Alcance Libre** el archivo **http://www.alcancelibre.org/linux/secrets/amavisd.te**:

```
wget http://www.alcancelibre.org/linux/secrets/amavisd.te
```

Editar el archivo **amavisd.te**:

```
vim amavisd.te
```

Verificar que el archivo **amavisd.te** tenga el siguiente contenido:

```


module amavisd 1.0;

require {
         type traceroute_port_t;
         type amavis_t;
         type clamd_t;
         type spamd_t;
         type initrc_var_run_t;
         type amavis_var_run_t;
         type root_t;
         class dir { write search add_name };
         class lnk_file read;
         class udp_socket name_bind;
         class file { ioctl append read lock };
}

#============= amavis_t ==============
allow amavis_t initrc_var_run_t:file { read lock };
```

```
allow amavis_t traceroute_port_t:udp_socket name_bind;

#============= clamd_t ==============
allow clamd_t amavis_var_run_t:dir { write search add_name };

#============= spamd_t ==============
allow spamd_t root_t:file { ioctl append };
```

Crear el archivo de módulo **amavisd.mod** a partir del archivo **amavisd.te**:

```
checkmodule -M -m -o amavisd.mod amavisd.te
```

Crear el archivo de política **amavisd.pp** a partir del archivo **amavisd.mod**

```
semodule_package -o amavisd.pp -m amavisd.mod
```

Incluir la política al sistema:

```
semodule -i /usr/share/selinux/packages/amavisd/amavisd.pp
```

66.3.2. Configuración de Amavisd-new.

Editar el archivo /**etc/amavisd/amavisd.conf**

```
vim /etc/amavisd/amavisd.conf
```

Localizar la siguiente línea:

```
$mydomain = 'example.com'; # a convenient default for other settings
```

Cambiar por lo siguiente:

```
$mydomain = 'dominio.com'; # a convenient default for other settings
```

66.3.3. Configuración de Postfix.

Editar el archivo /**etc/postfix/master.cf**

```
vim /etc/postfix/master.cf
```

Añadir al final de éste todo lo siguiente:

```
# Configuración de amavisd-new
amavisfeed unix    -       -       n        -      2     lmtp
    -o lmtp_data_done_timeout=1200
    -o lmtp_send_xforward_command=yes
    -o disable_dns_lookups=yes
    -o max_use=20
127.0.0.1:10025 inet n    -       n       -       -     smtpd
    -o content_filter=
    -o smtpd_delay_reject=no
    -o smtpd_client_restrictions=permit_mynetworks,reject
    -o smtpd_helo_restrictions=
    -o smtpd_sender_restrictions=
    -o smtpd_recipient_restrictions=permit_mynetworks,reject
    -o smtpd_data_restrictions=reject_unauth_pipelining
```

```
    -o smtpd_end_of_data_restrictions=
    -o smtpd_restriction_classes=
    -o mynetworks=127.0.0.0/8
    -o smtpd_error_sleep_time=0
    -o smtpd_soft_error_limit=1001
    -o smtpd_hard_error_limit=1000
    -o smtpd_client_connection_count_limit=0
    -o smtpd_client_connection_rate_limit=0
    -o receive_override_options=no_header_body_checks,no_unknown_recipient_checks,no_milters,no_address
_mappings
    -o local_header_rewrite_clients=
    -o smtpd_milters=
    -o local_recipient_maps=
    -o relay_recipient_maps=
```

Editar el archivo /**etc/postfix/main.cf**:

```
vim /etc/postfix/main.cf
```

Añadir al final de éste lo siguiente:

```
content_filter = amavisfeed:[127.0.0.1]:10024
```

Lo anterior se puede definir automáticamente en el archivo /**etc/postfix/main.cf** ejecutando:

```
postconf -e 'content_filter = amavisfeed:[127.0.0.1]:10024'
```

Editar el archivo /**etc/aliases**:

```
vim /etc/aliases
```

Definir un alias para la cuenta **virusalert**:

```
virusalert: fulano
```

Para que surtan efecto los cambios, ejecutar:

```
postalias /etc/aliases
```

66.3.4. Iniciar, detener y reiniciar el servicio spamass-milter.

Añadir los servicios **clamd.amavisd** y **amavisd** a los servicios de arranque del sistema:

```
chkconfig clamd.amavisd on
chkconfig amavisd on
```

Iniciar los servicios **clamd.amavisd** y **amavisd**:

```
service clamd.amavisd start
service amavisd start
```

Reiniciar el servicio **postfix**:

```
service postfix restart
```

66.3.5. Postfix con dominios virtuales y Amavisd-new.

Para poder utilizar Postfix **con dominios virtuales** y Amavisd-new, es indispensable editar el archivo /**etc/amavisd/amavisd.conf**:

```
vim /etc/amavisd/amavisd.conf
```

Y modificar los valores del parámetro @**local_domains_maps**. El valor predeterminado es el siguiente:

```
@local_domains_maps = ( [".$mydomain"] );
```

Se deben agregar los dominios virtuales de la siguiente manera:

```
@local_domains_maps = ( [".$mydomain", "dominio.com", "otrodominio.net", "otrodominio.org"] );
```

Y para que surtan efecto los cambios, se debe reiniciar el servicio **amavisd**:

```
service amavisd restart
```

67. Cómo configurar Postfix en CentOS para utilizar dominios virtuales con usuarios del sistema.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales (incluyendo su publicación, a través de cualquier medio, por entidades con fines de lucro). c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en castellano. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

67.1. Introducción.

Este documento permitirá configurar Postfix para utilizar múltiples dominios virtuales, utilizando los usuarios locales del sistema. Se requiere haber configurado previamente Postfix de la forma en que se describe en el documento titulado *«Cómo instalar y configurar Postfix en CentOS con soporte para TLS y autenticación.»* Se recomienda leer, estudiar y aplicar también los procedimientos descritos en el documento titulado *«Cómo instalar y configurar Amavisd-new con Postfix en CentOS.»*

67.2. Procedimientos.

67.2.1. Ajustes en el servicio saslauthd.

Si los usuarios se van a dar de alta siguiendo el formato *usuario@dominio.tld* en lugar de sólo *usuario*, una práctica común en los servidores con múltiples dominios virtuales, es necesario añadir al servicio **saslauthd** la opción **-r**, la cual permite combinar el nombre de usuario y dominio antes de pasar por el mecanismo de autenticación. Si éste es el caso, se debe editar el archivo **/etc/sysconfig/saslauthd**:

```
vim /etc/sysconfig/saslauthd
```

Y añadir la opción **-r** a los argumentos de **FLAGS**:

```
# Directory in which to place saslauthd's listening socket, pid file, and so
# on.  This directory must already exist.
SOCKETDIR=/var/run/saslauthd

# Mechanism to use when checking passwords.  Run "saslauthd -v" to get a list
# of which mechanism your installation was compiled with the ablity to use.
MECH=pam

# Options sent to the saslauthd. If the MECH is other than "pam" uncomment
# the next line.
# DAEMONOPTS=--user saslauth

# Additional flags to pass to saslauthd on the command line.  See saslauthd(8)
# for the list of accepted flags.
FLAGS=-r
```

Y reiniciar el servicio **saslauthd**.

```
service saslauthd restart
```

67.2.2. Configuración de SELinux.

Por lo general, la mayoría de los documentos disponibles en Internet recomiendan desactivar SELinux, sin mayores argumento o explicaciones. Sin embargo, hacer ésto implica renunciar a una magnífica protección que brinda al sistema esta importante implementación de seguridad. Tengo un lema personal que me gusta citar para explicar mi opinión respecto de SELinux:

> *Más vale tenerlo y jamás necesitarlo, que necesitarlo y carecer de éste.*

Si es posible utilizar SELinux junto con dominios virtuales. Cuando se quiere implementar un servicio de hospedaje con dominios virtuales y se utiliza **/home** para crear los directorios de inicio de los dominios virtuales, se requieren pocos o ningún ajuste en SELinux. Sin embargo, hay escenarios donde se utiliza **/var/www** para crear los directorios de inicio de los dominios virtuales. Sí se hace de este modo y sí se quiere mantener SELinux activo, es necesario generar una política que permita a los servicios de Postfix o Sendmail, Dovecot, Pyzor y Spamassassin poder realizar lectura, escritura y otros atributos sobre directorios y archivos con contexto **httpd_sys_content_t**. El siguiente procedimiento sirve para crear la política necesaria.

67.2.2.1. Procedimiento para crear política.

Crear el directorio **/usr/share/selinux/packages/virtualmail**:

```
mkdir /usr/share/selinux/packages/virtualmail
```

Cambiarse al directorio **/usr/share/selinux/packages/virtualmail**:

```
cd /usr/share/selinux/packages/virtualmail
```

Descargar desde **Alcance Libre** el archivo **http://www.alcancelibre.org/linux/secrets/virtualmail.te**:

```
wget http://www.alcancelibre.org/linux/secrets/virtualmail.te
```

Editar el archivo **virtualmail.te**:

```
vim virtualmail.te
```

Verificar que el archivo **virtualmail.te** tenga el siguiente contenido:

```
module virtualmail 1.0;

require {
	type pyzor_t;
	type sendmail_t;
	type postfix_local_t;
	type postfix_postdrop_t;
	type postfix_master_t;
	type procmail_t;
	type spamc_t;
	type dovecot_t;
	type tmp_t;
	type httpd_log_t;
	type httpd_sys_content_t;
	type httpd_config_t;
	type spamd_t;
	type system_mail_t;
	class fifo_file write;
	class file { read lock rename create write getattr link unlink append };
	class dir { search read write getattr remove_name add_name };
}

#============= dovecot_t ==============
allow dovecot_t httpd_sys_content_t:dir { write search read remove_name getattr add_name };
allow dovecot_t httpd_sys_content_t:file { write getattr link rename read lock create unlink };

#============= postfix_local_t ==============
allow postfix_local_t httpd_sys_content_t:dir search;

#============= postfix_postdrop_t ==============
allow postfix_postdrop_t tmp_t:file { getattr append };
allow postfix_postdrop_t httpd_log_t:file getattr;

#============= postfix_master_t ==============
allow postfix_master_t httpd_config_t:dir search;

#============= procmail_t ==============
allow procmail_t httpd_sys_content_t:dir search;

#============= pyzor_t ==============
allow pyzor_t httpd_sys_content_t:dir { write search };

#============= spamc_t ==============
allow spamc_t sendmail_t:fifo_file write;

#============= spamd_t ==============
allow spamd_t httpd_sys_content_t:dir { write search getattr };
allow spamd_t httpd_sys_content_t:file { read getattr };

#============= system_mail_t ==============
allow system_mail_t httpd_sys_content_t:file append;
```

Crear el archivo de módulo **virtualmail.mod** a partir del archivo **virtualmail.te**:

```
checkmodule -M -m -o virtualmail.mod virtualmail.te
```

Crear el archivo de política **virtualmail.pp** a partir del archivo **virtualmail.mod**

```
semodule_package -o virtualmail.pp -m virtualmail.mod
```

Incluir la politica al sistema:

```
semodule -i /usr/share/selinux/packages/virtualmail/virtualmail.pp
```

67.2.3. Configuración de Postfix.

67.2.3.1. Archivo /etc/postfix/main.cf.

Editar el archivo **/etc/postfix/main.cf**:

```
vim /etc/postfix/main.cf
```

Definir los siguientes parámetros:

```
# Establecer el valor de myhostname como localhost.localdomain
# También se puede definir cualquier otro dominio, siempre y cuando sea distinto
# a cualquiera de los definidos en los valores de virtual_alias_domains o en
# virtual_alias_maps.
myhostname = localhost.localdomain

# Definir el valor predeterminado para mydomain
mydomain = localhost.localdomain

# Definir los valores predeterminados para mydestination y relay_domains
mydestination = $myhostname, localhost.$mydomain, localhost
relay_domains = $mydestination

# Recomendado.
# Junto con virtual_alias_maps, reemplaza a virtual_maps
# Se utiliza para declarar los dominios virtuales.
# Se puede prescindir de éste si se añaden dominios en /etc/postfix/virtual.
virtual_alias_domains = $virtual_alias_maps

# Obligatorio.
# Junto con virtual_alias_domains, reemplaza a virtual_maps
# Se utiliza para declarar la reescritura de direcciones. Ejemplo:
# jbarrios@dominio.com  joel
# Ejemplo hace que todo correo para joel@dominio.com se entregue a joel
# Si se quiere precindir de utilizar virtual_alias_domains, añadir también los
# dominios en este formato:
# dominio.com           dominio.com
# otrodominio.net       otrodominio.net
# otrodominio.org       otrodominio.org
# Si se hace lo anterior, comentar virtual_alias_domains.
virtual_alias_maps = hash:/etc/postfix/virtual

# Recomendado.
# Es la contraparte de alias_database = /etc/aliases
# Se utiliza para reescritura de direcciones de salida. Ejemplo:
# joel          joel.barrios
# Ejemplo hace que todo el correo de joel salga como joel.barrios
canonical_maps = hash:/etc/postfix/canonical

# Recomendado.
# Se utiliza solo para reescribir la dirección de salida de una cuenta.
# Ejemplo:
# joel          jbarrios@dominio.com
# Ejemplo hace que todo el correo de joel salga como jbarrios@dominio.com
sender_canonical_maps = hash:/etc/postfix/sender_canonical

# Opcional.
# Poco utilizado. Utilizar virtual_alias_maps en su lugar.
# Considerar que se procesa antes que canonical_maps.
# Se utiliza solo para reescribir solo la dirección de entrada de una cuenta.
# Ejemplo:
# jbarrios@dominio.com          joel
# Ejemplo hace que todo correo para jbarrios@dominio.com se entregue a joel
recipient_canonical_maps = hash:/etc/postfix/recipient_canonical
```

Todo lo anterior se puede realizar también ejecutando el mandato **postconf** para cada parámetro:

```
postconf -e 'myhostname = localhost.localdomain'
postconf -e 'mydomain = localhost.localdomain'
postconf -e 'mydestination = $myhostname, localhost.$mydomain, localhost'
postconf -e 'relay_domains = $mydestination'
postconf -e 'virtual_alias_domains = $virtual_alias_maps'
postconf -e 'virtual_alias_maps = hash:/etc/postfix/virtual'
postconf -e 'canonical_maps = hash:/etc/postfix/canonical'
postconf -e 'sender_canonical_maps = hash:/etc/postfix/sender_canonical'
postconf -e 'recipient_canonical_maps = hash:/etc/postfix/recipient_canonical'
```

Al terminar, genere los archivos **/etc/postfix/sender_canonical** y **/etc/postfix/recipient_canonical**:

```
touch /etc/postfix/sender_canonical
touch /etc/postfix/recipient_canonical
```

67.2.3.2. Archivos /etc/postfix/virtual y /etc/postfix/sender_canonical.

Editar el archivo **/etc/postfix/virtual**:

```
vim /etc/postfix/virtual
```

Crear la tabla de cuentas de correo electrónico virtuales de entrada, especificando a que cuenta de usuario local se entrega cada dirección.

```
dominio.com                    dominio.com
otrodominio.net                otrodominio.net
otrodominio.org                otrodominio.org
joel@dominio.com               joel
juan@dominio.com               juan
pablo@dominio.com              pablo
pedro@dominio.com              pedro
hugo@otrodominio.net           hugo
luis@otrodominio.org           luis
webmaster@dominio.com          joel@dominio.com
webmaster@otrodominio.net      hugo@otrodominio.net
webmaster@otrodominio.org      luis@otrodominio.org
```

Editar el archivo **/etc/postfix/sender_canonical**:

```
vim /etc/postfix/sender_canonical
```

Crear la tabla de cuentas de correo electrónico virtuales de salida, especificando las direcciones de salida que utilizará cada usuario. Es decir, casi lo contrario a lo establecido en /etc/postfix/virtual, pero especificando un único usuario para cada cuenta de correo electrónico. Jamás se especifique más de un usuario por cuenta de correo electrónico, ni más de una cuenta de correo electrónico por usuario.

```
joel            joel@dominio.com
juan            juan@dominio.com
pablo           pablo@dominio.com
pedro           pedro@dominio.com
hugo            hugo@otrodominio.net
luis            luis@otrodominio.org
```

Utilizar el mandato **postmap** con los archivos **/etc/postfix/canonical**, **/etc/postfix/recipient_canonical**, **/etc/postfix/sender_canonical** y **/etc/postfix/virtual** a fin de generar los archivos .db correspondientes y que surtan efecto los cambios luego de reiniciar el servicio **postfix**:

```
postmap /etc/postfix/canonical
postmap /etc/postfix/recipient_canonical
postmap /etc/postfix/sender_canonical
postmap /etc/postfix/virtual
```

67.2.4. Reiniciar el servicio postfix.

A fin de que surtan efecto todos los cambios, se debe reiniciar el servicio **postfix**:

```
service postfix restart
```

68. Envío de correo a todos los usuarios del sistema.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

68.1. Procedimientos

1. Lo primero será generar un archivo en el sistema, el cual tendrá como contenido una lista de los usuarios del sistema a los que se quiere enviar un mensaje. Éste puede localizarse en cualquier lugar del sistema, como por ejemplo `/etc/mail/allusers`. Puede editarse el archivo `/etc/mail/allusers` y añadir individualmente cada usuario que se desee conforme esa lista o bien, si se quiere añadir a todos los usuarios del sistema, ejecutar lo siguiente:

```
awk -F: '$3 > 500 { print $1 }' /etc/passwd > /etc/mail/allusers
```

2. A continuación, debe modificarse el archivo `/etc/aliases` y añadir al final del mismo:

```
allusers: :include:/etc/mail/allusers
```

1. Al terminar sólo debe ejecutarse el mandato `newaliases` o bien reiniciar el servicio de Sendmail (el guión de inicio se encarga de hacer todo lo necesario).

3. Para probar, bastará con enviar un mensaje de correo electrónico a la cuenta `allusers` del servidor.

68.2. Acerca de la seguridad

Evite a toda costa utilizar **allusers** o palabras muy obvias como alias de correo para enviar a todas las cuentas. Seguramente quienes se dedican a enviar correo masivo no solicitado o correo chatarra (*Spam*), tratarán de enviar correo a este alias en el servidor. No les facilite el trabajo a esas personas y trate de utilizar un alias ofuscado o en clave. Ejemplo: *8jj37sjei876*.

69. Cómo configurar clamav-milter.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

69.1. Introducción.

69.1.1. Acerca de clamav-milter.

Clamav-milter es un componente para añadir (**Plug-in**) para la biblioteca de filtros de correo (**libmilter**) de **Sendmail**, que se encarga de hacer pasar todo el correo entrante, incluyendo todo lo que se reciba a través de **rmail/UUCP**, a través del **ClamAV**, que a su vez es un poderoso y robusto motor, con licenciamiento libre, para la detección de gusanos, troyanos y virus. Verifica el correo electrónico durante la conexión con el servidor de correo que remite éste ultimo y lo rechaza automáticamente si éste incluye algún gusanos, troyanos o virus.

Al igual que **clamav-milter**, el cual es utilizado para la filtración de Spam, representa una excelente alternativa pues tiene un bajo consumo de recursos de sistema, haciéndolo idóneo para servidores con sustento físico obsoleto o donde otras aplicaciones tiene mayor prioridad en la utilización de recursos de sistema.

URL: http://www.clamav.net/

69.1.2. Acerca de ClamAV.

ClamAV es un conjunto de herramientas antivirus, libre y de código fuente abierto, que tiene las siguiente características:

- Distribuido bajo los términos de la Licencia Publica General GNU versión 2.
- Cumple con las especificaciones de familia de estándares **POSIX** (**P**ortable **O**perating **S**ystem **I**nterface for UNI**X** o interfaz portable de sistema operativo para Unix).
- Exploración rápida.
- Detecta más de 720 mil virus, gusanos y troyanos, incluyendo virus para MS Office.
- Capacidad para examinar contenido de archivos ZIP, RAR, Tar, Gzip, Bzip2, MS OLE2, MS Cabinet, MS CHM y MS SZDD.
- Soporte para explorar archivos comprimidos con UPX, FSG y Petite.
- Avanzada herramienta de actualización con soporte para firmas digitales y consultas basadas sobre DNS.

URL: http://www.clamav.net/

69.2. Equipamiento lógico necesario.

- sendmail (previamente configurado)
- make
- sendmail-cf
- m4

- clamav
- clamav-milter

69.2.1. Creación del usuario para ClamAV.

De modo predeterminado, en los paquetes RPM basados sobre los disponibles para Fedora, el usuario para ClamAV se asigna a través de los mandatos **fedora-groupadd** y **fedora-useradd** el UID y GID 4 en el sistema. A fin de prevenir un conflicto de UID/GID con otros usuarios y grupos de sistema, se recomienda crear previamente al grupo y usuario correspondientes para ClamAV:

```
groupadd -r clamav
useradd -r -s /sbin/nologin -d /var/lib/clamav -M -c 'Clamav Antivirus' -g clamav clamav
```

69.2.2. Instalación a través de yum.

Si dispone de un servidor con **CentOS 5** y **6** o **Red Hat™ Enterprise Linux 5** y **6**, puede utilizar el el almacén YUM de **Alcance Libre** para servidores en producción, descargando el archivo **http://www.alcancelibre.org/al/server/AL-Server.repo** dentro del directorio **/etc/yum.repos.d/**:

```
cd /etc/yum.repos.d/
wget -N http://www.alcancelibre.org/al/server/AL-Server.repo
cd
```

Este archivo, que se guarda como **/etc/yum.repos.d/AL-Server.repo**, debe tener el siguiente contenido:

```
[AL-Server]
name=AL Server para Enterprise Linux $releasever
mirrorlist=http://www.alcancelibre.org/al/el$releasever/al-server
gpgcheck=1
gpgkey=http://www.alcancelibre.org/al/AL-RPM-KEY
```

La instalación a través del mandato **yum** requiere utilizar lo siguiente:

```
yum -y install clamav-milter clamav-milter-sysv clamav-data-empty clamav-update
clamav-scanner clamav-scanner-sysvinit
```

69.3. Procedimientos.

69.3.1. SELinux y el servicio clamav-milter.

69.3.1.1. CentOS 5 y Red Hat Enterprise Linux 5.

En CentOS 5 ,y Red Hat Enterprise Linux 5 se debe crear una política para permitir al servicio **clamd.scan** utilizar **JIT** y la función *execmem()*.

Genere un nuevo directorio denominado **/usr/share/selinux/packages/clamd**:

```
mkdir /usr/share/selinux/packages/clamd
```

Cambiarse al directorio **/usr/share/selinux/packages/clamd**:

```
cd /usr/share/selinux/packages/clamd
```

Descargar el archivo **http://www.alcancelibre.org/linux/secrets/clamd.te**:

```
wget http://www.alcancelibre.org/linux/secrets/clamd.te
```

Editar el archivo recién descargado:

```
vim clamd.te
```

Asegurarse que tenga el siguiente contenido:

```
module clamd 1.0;

require {
        type clamd_t;
        class process execmem;
}

#============= clamd_t ==============
allow clamd_t self:process execmem;
```

Lo anterior fue obtenido de la salida del mandato **cat /var/log/audit/audit.log|grep audit|audit2allow -m clamd>clamd.te** en un sistema donde SELinux impedía a **clamav-milter** utilizar la función *execmem()*.

A continuación, se genera un el archivo de módulo para SELinux (**clamd.mod**) utilizando el mandato **checkmodule** de la siguiente forma:

```
checkmodule -M -m -o clamd.mod clamd.te
```

Luego, se procede a empaquetar el archivo **clamd.mod** como el archivo **clamd.pp**:

```
semodule_package -o clamd.pp -m clamd.mod
```

Finalmente se vincula el archivo **clamd.pp** obtenido con las políticas actuales de SELinux y se cargan éstas en el núcleo en ejecución:

```
semodule -i /usr/share/selinux/packages/clamd/clamd.pp
```

Una vez cargadas las nuevas políticas, se pueden eliminar los archivos **clamd.te** y **clamd.mod**, pues solo será necesario que exista el archivo binario **clamd.pp**.

A fin de evitar realizar todo lo anterior, permitir que el servicio **clamd.scan** pueda utilizar la función *execmem()* y que SELinux impida las conexiones del servicio **clamav-milter** hacia el servicio **clamd.scan**, utilice el siguiente mandato:

```
setsebool -P clamd_disable_trans 1
```

Para que SELinux permita al servicio **clamav-milter** funcionar normalmente y que permita realizar la revisión de correo electrónico, utilice el siguiente mandato:

```
setsebool -P clamscan_disable_trans 1
```

Para que SELinux permita al mandato **freshclam** funcionar normalmente y que permita actualizar la base de datos de firmas digitales, utilice el siguiente mandato:

```
setsebool -P freshclam_disable_trans 1
```

69.3.1.2. CentOS 6 y Red Hat Enterprise Linux 6.

En CentOS 6 y Red Hat Enterprise Linux 6 solo existe una política a configurar y es **clamd_use_jit**, la cual permite al servicio **clamd.scan** utilizar **JIT** y la función *execmem()*.

```
setsebool -P clamd_use_jit on
```

69.3.2. Requisitos previos.

Se requiere un servidor de correo con **Sendmail**, previamente configurado y funcionando para enviar y recibir correo electrónico. Para más detalles al respecto, consultar el documento titulado *«Configuración básica de Sendmail (Parte I).»*.

69.3.3. Archivo /etc/mail/sendmail.mc.

Es necesario agregar el siguiente contenido en el archivo **/etc/mail/sendmail.mc**, justo arriba de la línea **MAILER(smtp)dnl**.

```
INPUT_MAIL_FILTER(`clamav', `S=local:/var/run/clamav-milter/clamav.sock, F=, T=S:4m;R:4m')dnl
define(`confINPUT_MAIL_FILTERS', `clamav')dnl
```

Si se combina con **Spamassassin Milter**, quedaría del siguiente modo:

```
INPUT_MAIL_FILTER(`clamav', `S=local:/var/run/clamav-milter/clamav.sock, F=, T=S:4m;R:4m')dnl
INPUT_MAIL_FILTER(`spamassassin', `S=unix:/var/run/spamass-milter/spamass-milter.sock, F=,
T=C:15m;S:4m;R:4m;E:10m')dnl
define(`confMILTER_MACROS_CONNECT',`t, b, j, _, , , ')dnl
define(`confMILTER_MACROS_HELO',`s, , , , , ')dnl
define(`confINPUT_MAIL_FILTERS', `spamassassin,clamav')dnl
```

69.3.4. Configuración.

Clamav-milter depende totalmente de la base de datos de **ClamAV**. El funcionamiento estándar, que consiste en rechazar correo electrónico que contenga virus y otros programas malignos, funciona sin necesidad de parámetros adicionales. Las banderas de inicio para clamav-milter están definidas en el archivo **/etc/sysconfig/clamav-milter**, mismo que permite funcionar normalmente sin necesidad de modificar un solo parámetro, a menos que se necesite especificar alguna opción avanzada definida en la página de manual de clamav-milter.

```
man clamav-milter
```

69.3.5. Iniciar, detener y reiniciar el servicio clamav-milter.

Desde la versión 0.95, ClamAV-milter requiere esté funcionando clamdscan como servicio. Los paquetes de ClamAV incluyen lo necesario a través de clamav-scanner. Solo se requiere agregar al arranque del sistema y se inicia los servicios **clamd.scan** y **clamav-milter** del siguiente modo y orden:

```
chkconfig clamd.scan on
service clamd.scan start
chkconfig clamav-milter on
service clamav-milter start
```

El archivo **/etc/freshclam.conf** de los paquetes distribuidos por **Alcance Libre** ya incluye las modificaciones necesarias para permitir el funcionamiento del mandato **freshclam**. Sin embargo, si se utilizan paquetes para Fedora, es necesario editar este archivo y comentar o eliminar la línea 9, que incluye simplemente la palabra inglesa *Example* y que de otro mod impediría utilizar el mandato **freshclam**:

```
##
## Example config file for freshclam
## Please read the freshclam.conf(5) manual before editing this file.
##


# Comment or remove the line below.
# Example
```

El archivo **/etc/sysconfig/freshclam** de los paquetes distribuidos por **Alcance Libre** ya incluye las modificaciones necesarias para permitir la actualización automática de la base de datos de **ClamAV**. Si se utilizan paquetes de Fedora y a fin de mantener actualizada la base de datos de firmas digitales, es necesario editar el archivo **/etc/sysconfig/freshclam** con el objeto de permitir las actualizaciones automáticas:

```
### !!!!! REMOVE ME !!!!!!
### REMOVE ME: By default, the freshclam update is disabled to avoid
### REMOVE ME: network access without prior activation
# FRESHCLAM_DELAY=disabled-warn # REMOVE ME
```

Antes de poner en operación el servidor, es recomendable actualizar manualmente y de manera inmediata, la base de datos de firmas utilizando el mandato **freshclam**, desde cualquier terminal como **root**.

```
freshclam
```

Al terminar, considerando que está instalado el paquete **sendmail-mc**, el cual permite reconfigurar **Sendmail** a partir del archivo **/etc/mail/sendmail.mc**, se debe reiniciar el servicio **sendmail** para que surtan efectos los cambios.

```
service sendmail restart
```

70. Cómo configurar spamass-milter.

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

70.1. Introducción.

70.1.1. Requisitos previos.

Se requiere un servidor de correo con **Sendmail**, previamente configurado y funcionando para enviar y recibir correo electrónico. Para más detalles al respecto, consultar el documento titulado *«Configuración básica de Sendmail»*.

Se requiere además leer y estudiar previamente la información del documento titulado *«Cómo instalar y configurar Spamassassin.»*

70.1.2. Acerca de spamass-milter.

Spamass-milter es un componente adicional (**Plug-in**) para la biblioteca de filtros de correo (**libmilter**) de **Sendmail**, que se encarga de hacer pasar todo el correo entrante, incluyendo todo lo que se reciba a través de **rmail/UUCP**, a través de **SpamAssassin**, que a su vez es un poderoso y robusto componente de filtrado de correo.

Representa una excelente alternativa pues tiene un bajo consumo de recursos de sistema, haciéndolo idóneo para servidores con sustento físico obsoleto o donde otras aplicaciones tiene mayor prioridad en la utilización de recursos de sistema.

URL: http://savannah.nongnu.org/projects/spamass-milt/

70.1.3. Acerca de SpamAssassin.

SpamAssassin es una implementación que utiliza un sistema de puntuación, basado sobre algoritmos de tipo genético, para identificar mensajes que pudieran ser sospechosos de ser correo masivo no solicitado, añadiendo cabeceras a los mensajes de modo que puedan ser filtrados por el cliente de correo electrónico o **MUA** (**M**ail **U**ser **A**gent).

URL: http://spamassassin.apache.org/

70.2. Equipamiento lógico necesario.

- sendmail (previamente configurado)
- make
- spamassassin
- perl-Mail-SPF
- sendmail-cf
- m4
- spamass-milter
- perl-Razor-Agent

- pyzor

70.2.1. Instalación a través de yum.

Si dispone de un servidor con **CentOS 4** o **5** o bien **Red Hat™ Enterprise Linux 4** o **5**, puede utilizar el depósito yum de **Alcance Libre** para servidores en producción:

```
[AL-Server]
name=AL Server para Enterprise Linux $releasever
mirrorlist=http://www.alcancelibre.org/al/el$releasever/al-server
gpgcheck=1
gpgkey=http://www.alcancelibre.org/al/AL-RPM-KEY
```

La instalación solo requiere utilizar lo siguiente:

```
yum -y install spamass-milter perl-Mail-SPF perl-Razor-Agent pyzor
```

70.3. Procedimientos.

70.3.1. SELinux y el servicio spamass-milter.

A fin de que SELinux permita al servicio **spamassassin** conectarse a servicios externos, como razor o Pyzor, utilice el siguiente mandado:

```
setsebool -P spamassassin_can_network 1
```

A fin de que SELinux permita a los usuarios del sistema utilizar **spamassassin** desde sus directorios de inicio, utilice el siguiente mandato:

```
setsebool -P spamd_enable_home_dirs 1
```

Si se desea desactivar toda gestión de SELinux sobre los servicios **spamass-milter** y **spamassassin**, haciendo que todo lo anterior pierda sentido y eliminando la protección que brinda esta implementación, utilice los siguientes mandatos:

```
setsebool -P spamd_disable_trans 1
setsebool -P spamass_milter_disable_trans 1
```

70.3.1.1. Ajustes adicionales.

Actualizaciones recientes en las políticas de SELinux impedirán que el servicio **spamass-milter** pueda siquiera iniciar. Por lo tanto, es imperativo instalar las políticas de SELinux correspondientes.

Genere un nuevo directorio denominado **/usr/share/selinux/packages/spamassmilter**:

```
mkdir /usr/share/selinux/packages/spamassmilter
```

Cambiarse al directorio **/usr/share/selinux/packages/spamassmilter**:

```
cd /usr/share/selinux/packages/spamassmilter
```

Si utiliza **CentOS 5** o **Red Hat Enterprise Linux 5**, descargar el archivo **http://www.alcancelibre.org/linux/secrets/el5/spamassmilter.te**:

```
wget http://www.alcancelibre.org/linux/secrets/el5/spamassmilter.te
```

Editar el archivo recién descargado:

```
vim spamassmilter.te
```

Asegurarse que tenga el siguiente contenido:

```
module spamassmilter 1.0;

require {
        type spamass_milter_data_t;
        type spamass_milter_t;
        type pyzor_t;
        type initrc_var_run_t;
        type spamd_t;
        class dir { search read create write getattr remove_name add_name };
        class file { read create ioctl write getattr unlink append };
}

#============= pyzor_t ==============
allow pyzor_t spamass_milter_data_t:dir { write search create getattr add_name };
allow pyzor_t spamass_milter_data_t:file { read write create getattr };

#============= spamass_milter_t ==============
allow spamass_milter_t initrc_var_run_t:file { write getattr };

#============= spamd_t ==============
allow spamd_t spamass_milter_data_t:dir { write search read remove_name create getattr add_name };
allow spamd_t spamass_milter_data_t:file { write getattr read create unlink ioctl append };
```

Lo anterior fue obtenido de la salida del mandato **cat /var/log/audit/audit.log|grep audit|audit2allow -m spamassmilter>spamassmilter.te** en un sistema **CentOS 5** donde SELinux impedía a **spamass-milter** funcionar correctamente.

Si utiliza **CentOS 6** o **Red Hat Enterprise Linux 6**, descargar el archivo **http://www.alcancelibre.org/linux/secrets/el6/spamassmilter.te**:

```
wget http://www.alcancelibre.org/linux/secrets/el6/spamassmilter.te
```

Editar el archivo recién descargado:

```
vim spamassmilter.te
```

Asegurarse que tenga el siguiente contenido:

```
module spamassmilter 1.0;

require {
        type spamass_milter_data_t;
        type spamass_milter_t;
        type pyzor_t;
        type initrc_var_run_t;
        type spamc_t;
        type spamd_t;
```

```
        class dir { search read create write open getattr remove_name add_name };
        class file { read create ioctl write open getattr unlink append };
}

#============= pyzor_t ==============
allow pyzor_t spamass_milter_data_t:dir { write search create getattr add_name };
allow pyzor_t spamass_milter_data_t:file { read write create getattr };

#============= spamass_milter_t ==============
allow spamass_milter_t initrc_var_run_t:file { write getattr };

#============= spamd_t ==============
allow spamd_t spamass_milter_data_t:dir { write open search read remove_name create getattr add_name };
allow spamd_t spamass_milter_data_t:file { write open getattr read create unlink ioctl append };

#============= spamc_t ==============
allow spamc_t spamass_milter_data_t:file open;
```

Lo anterior fue obtenido de la salida del mandato **cat /var/log/audit/audit.log|grep audit|audit2allow -m spamassmilter>spamassmilter.te** en un sistema **CentOS 6** donde SELinux impedía a **spamass-milter** funcionar correctamente.

A continuación, se genera un el archivo de módulo para SELinux (**spamassmilter.mod**) utilizando el mandato **checkmodule** de la siguiente forma:

```
checkmodule -M -m -o spamassmilter.mod spamassmilter.te
```

Luego, se procede a empaquetar el archivo **spamassmilter.mod** como el archivo **spamassmilter.pp**:

```
semodule_package -o spamassmilter.pp -m spamassmilter.mod
```

Finalmente se vincula el archivo **spamassmilter.pp** obtenido con las políticas actuales de SELinux y se cargan éstas en el núcleo en ejecución:

```
semodule -i /usr/share/selinux/packages/spamassmilter/spamassmilter.pp
```

Una vez cargadas las nuevas políticas, se pueden eliminar los archivos **spamassmilter.te** y **spamassmilter.mod**, pues solo será necesario que exista el archivo binario **spamassmilter.pp**.

70.3.2. Archivo /etc/mail/sendmail.mc.

Editar el archivo **/etc/mail/sendmail.mc**:

```
vim /etc/mail/sendmail.mc
```

Es necesario agregar el siguiente contenido en el archivo **/etc/mail/sendmail.mc**, justo arriba de **MAILER(smtp)dnl**.

```
dnl MASQUERADE_DOMAIN(localhost)dnl
dnl MASQUERADE_DOMAIN(localhost.localdomain)dnl
dnl MASQUERADE_DOMAIN(mydomainalias.com)dnl
dnl MASQUERADE_DOMAIN(mydomain.lan)dnl
INPUT_MAIL_FILTER(`spamassassin', `S=unix:/var/run/spamass-milter/spamass-milter.sock, F=,
T=C:15m;S:4m;R:4m;E:10m')dnl
define(`confMILTER_MACROS_CONNECT',`t, b, j, _, {daemon_name}, {if_name}, {if_addr}')dnl
define(`confMILTER_MACROS_HELO',`s, {tls_version}, {cipher}, {cipher_bits}, {cert_subject},
{cert_issuer}')dnl
define(`confMILTER_MACROS_ENVRCPT',`r, v, Z')dnl
MAILER(smtp)dnl
MAILER(procmail)dnl
```

```
dnl MAILER(cyrusv2)dnl
```

Si se combina con **ClamAV Milter**, quedaría del siguiente modo:

```
dnl MASQUERADE_DOMAIN(localhost)dnl
dnl MASQUERADE_DOMAIN(localhost.localdomain)dnl
dnl MASQUERADE_DOMAIN(mydomainalias.com)dnl
dnl MASQUERADE_DOMAIN(mydomain.lan)dnl
INPUT_MAIL_FILTER(`clamav', `S=local:/var/run/clamav-milter/clamav.sock, F=, T=S:4m;R:4m')dnl
INPUT_MAIL_FILTER(`spamassassin', `S=unix:/var/run/spamass-milter/spamass-milter.sock, F=,
T=C:15m;S:4m;R:4m;E:10m')dnl
define(`confMILTER_MACROS_CONNECT',`t, b, j, _, {daemon_name}, {if_name}, {if_addr}')dnl
define(`confMILTER_MACROS_HELO',`s, {tls_version}, {cipher}, {cipher_bits}, {cert_subject},
{cert_issuer}')dnl
define(`confMILTER_MACROS_ENVRCPT',`r, v, Z')dnl
define(`confINPUT_MAIL_FILTERS', `spamassassin,clamav')dnl
MAILER(smtp)dnl
MAILER(procmail)dnl
dnl MAILER(cyrusv2)dnl
```

70.3.3. Archivo /etc/sysconfig/spamass-milter.

Editar el archivo **/etc/sysconfig/spamass-milter**:

```
vim /etc/sysconfig/spamass-milter
```

El archivo **/etc/sysconfig/spamass-milter** incluye el siguiente contenido:

```
### Override for your different local config
#SOCKET=/var/run/spamass-milter/spamass-milter.sock

### Standard parameters for spamass-milter are:
### -P /var/run/spamass-milter.pid (PID file)
###
### Note that the -f parameter for running the milter in the background
### is not required because the milter runs in a wrapper script that
### backgrounds itself
###
### You may add another parameters here, see spamass-milter(1)
#EXTRA_FLAGS="-m -r 15"
```

De forma predeterminada, a través del parámetro **-m**, **spamass-milter** desactiva la modificación del asunto del mensaje (**Subject:**) y la cabecera **Content-Type:**, lo cual es conveniente para añadir cabeceras y se procesado posteriormente, y, a través del parámetro **-r 15**, rechaza los mensajes de correo electrónico cuando éstos tienen asignados 15 puntos o más. Se pueden modificar el número de puntos mínimos para rechazar directamente el correo electrónico sospechoso de ser *Spam* incrementando el valor para el parámetro **-r**. La recomendación es asignar un valor mayor al definido en el archivo **/etc/mail/spamassassin/local.cf**. Si, por ejemplo, se establece en éste último **required_hits 4.5** y **rewrite_header Subject {Spam?}** y en el archivo **/etc/sysconfig/spamass-milter** se establece **EXTRA_FLAGS="-m -r 10"**, ocurrirá lo siguiente:

1. Todos los mensajes marcados con 4.4 puntos o menos, se entregarán inmediatamente al usuario sin modificaciones visibles.

2. Todos los mensajes marcados desde 4.5 hasta 9.9 puntos se entregarán al usuario con el asunto modificado añadiendo a éste {Spam?} al inicio.

3. Todos los mensajes que estén marcados con 10.0 puntos o más serán rechazados automáticamente.

Basado sobre el ejemplo mencionado, el contenido del archivo **/etc/sysconfig/spamass-milter** quedaría del siguiente modo:

```
### Override for your different local config
#SOCKET=/var/run/spamass-milter/spamass-milter.sock

### Standard parameters for spamass-milter are:
### -P /var/run/spamass-milter.pid (PID file)
###
### Note that the -f parameter for running the milter in the background
### is not required because the milter runs in a wrapper script that
### backgrounds itself
###
### You may add another parameters here, see spamass-milter(1)
EXTRA_FLAGS="-m -r 10"
```

70.3.4. Archivo /etc/procmailrc.

Si se desea que el correo marcado con una mínima puntuación para ser considerado **Spam** (igual o superior al valor definido para el parámetro **required_hits** del archivo /etc/mail/spamassassin/local.cf) se entregue en una carpeta diferente al buzón de entrada, para ser consultado a través de un webmail (Squirrelmail o GroupOffice) o bien un cliente con soporte IMAP (Microsoft Outlook, GNOME Evolution o Mozilla Thunderbird), se puede crear el archivo **/etc/procmailrc**:

```
vim /etc/procmailrc
```

Y añadirle el siguiente contenido:

```
# Hacer pasar el correo por spamassassin
:0fw
| /usr/bin/spamc

# Mover mensajes positivos a Spam hacia la capeta ~/mail/Spam del usuario
:0:
* ^X-Spam-Status: Yes
$HOME/mail/Spam
```

Lo anterior define una regla condicionada a que la cabecera del mensaje incluya **X-Spam-Status: Yes**, el cual es agregado por **SpamAssassin** cuando hay casos que superan el mínimo de puntos para ser considerado **Spam**, de modo que todo correo que incluya esta cabecera será almacenado en la carpeta **mail/Spam** propiedad del usuario a quien sea destinado el mensaje. Al estar en **/etc/procmailrc**, esta regla se aplica a todas la cuentas de usuario en el servidor. Combinado con todo lo anterior, ocurrirá lo siguiente:

1. Todos los mensajes marcados con 4.4 puntos o menos, se entregarán inmediatamente al usuario sin modificaciones visibles.

2. Todos los mensajes marcados desde 4.5 hasta 9.9 puntos se entregarán al usuario con el asunto modificado añadiendo a éste {Spam?} al inicio y se almacenarán en la capeta **~/mail/Spam** del usuario.

3. Todos los mensajes que estén marcados con 10.0 puntos o más serán rechazados automáticamente.

Archivo /etc/sysconfig/spamassassin.

A fin de que **spamass-milter** y **spamassassin** trabajen juntos, es necesario exista el directorio de configuración para el usuario **sa-milt** que se utilizará para iniciar **spamd**, el cual corresponde al servicio **spamassassin**. Por lo general, este directorio se crea automáticamente al instalar el paquete **spamassassin**.

Este directorio debe pertenecer al usuario **sa-milt** y grupo **sa-milt**.

```
chown -R sa-milt:sa-milt /var/lib/spamassassin
```

Se edita el archivo **/etc/sysconfig/spamassassin**:

```
vim /etc/sysconfig/spamassassin
```

Y se añaden las opciones **-u sa-milt -x --virtual-config-dir=/var/lib/spamassassin**, las cuales especifican que se iniciará como el usuario **sa-milt**, que se desactivará la configuración por usuario y que se utilizará **/var/lib/spamassassin** como directorio virtual de configuración. De tal modo, el archivo debe quedar de la siguiente forma:

```
# Options to spamd
SPAMDOPTIONS="-d -c -m5 -H -u sa-milt -x --virtual-config-dir=/var/lib/spamassassin"
```

70.3.5. Iniciar, detener y reiniciar el servicio spamass-milter.

Se agrega al arranque del sistema y se inicia el servicio **spamassasin** del siguiente modo:

```
chkconfig spamassassin on
service spamassassin start
```

El servicio **spamass-milter** se agrega al arranque del sistema y se inicia del siguiente modo:

```
chkconfig spamass-milter on
service spamass-milter start
```

Al terminar, considerando que está instalado el paquete **sendmail-mc**, el cual permite aplicar cambios en la configuración **Sendmail** a partir del archivo **/etc/mail/sendmail.mc**, se debe reiniciar el servicio **sendmail** para que surtan efectos los cambios realizado en el archivo mencionado.

```
service sendmail restart
```

A fin de mantener actualizado el juego de reglas y filtros de Spamassassin, es conveniente actualizar éstos de vez en cuando, a lo sumo una o dos veces al mes. Los juegos de reglas y filtros de Spamassassin realmente sufren pocos cambios a lo largo del año y se almacenan en un sub-directorio dentro de **/var/lib/spamassassin/**. Solo es necesario conservar el sub-directorio con la versión más reciente. El siguiente mandato realizará la consulta y actualización de reglas y filtros de Spamassassin y reiniciará el servicio solamente si se descargó una actualización:

```
sa-update && service spamassassin restart
```

71. Introducción a OpenLDAP.

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

71.1. Introducción.

71.1.1. Acerca de LDAP.

LDAP (**L**ightweight **D**irectory **A**ccess **P**rotocol) es un protocolo para consulta y modificación de servicios de directorio que se desempeñan sobre TCP/IP. **LDAP** utiliza el modelo X.500 para su estructura, es decir, se estructura árbol de entradas, cada una de las cuales consiste de un conjunto de atributos con nombre y que a su vez almacenan valores.

El inicio de la operación StartTLS en un servidor LDAP, establece la comunicación **TLS** (**T**ransport **L**ayer **S**ecurity o Seguridad para Nivel de Transporte) a través del mismo puerto 389 por TCP. Provee confidencialidad en el transporte de datos e protección de la integridad de datos. Durante la negociación, el servidor envía su certificado con estructura X.509 para verificar su identidad.

URL: http://en.wikipedia.org/wiki/LDAP

71.1.2. Acerca de RSA.

RSA, acrónimo de los apellidos de sus autores, Ron **R**ivest, Adi **S**hamir y Len **A**dleman, es un algoritmo para el ciframiento de claves públicas que fue publicado en 1977, patentado en EE.UU. en 1983 por el el Instituto Tecnológico de Michigan (**MIT**). **RSA** es utilizado ampliamente en todo el mundo para los protocolos destinados para el comercio electrónico.

URL: http://es.wikipedia.org/wiki/RSA

71.1.3. Acerca de X.509.

X.509 es un estándar **ITU-T** (estandarización de **T**elecomunicaciones de la **I**nternational **T**elecommunication **U**nion) para infraestructura de claves públicas (**PKI** o **P**ublic **K**ey **I**nfrastructure). Entre otras cosas, establece los estándares para certificados de claves públicas y un algoritmo para validación de ruta de certificación. Este último se encarga de verificar que la ruta de un certificado sea válida bajo una infraestructura de clave pública determinada. Es decir, desde el certificado inicial, pasando por certificados intermedios, hasta el certificado de confianza emitido por una Autoridad Certificadora (**CA** o **C**ertification **A**uthority).

URL: http://es.wikipedia.org/wiki/X.509

71.1.4. Acerca de OpenSSL.

OpenSSL es una implementación libre, de código abierto, de los protocolos **SSL** (**S**ecure **S**ockets **L**ayer o Nivel de Zócalo Seguro) y **TLS** (**T**ransport **L**ayer **S**ecurity o Seguridad para Nivel de Transporte). Está basado sobre el extinto proyecto **SSLeay**, iniciado por Eric Young y Tim Hudson, hasta que éstos comenzaron a trabajar para la división de seguridad de EMC Corporation.

URL: http://www.openssl.org/

72. Configuración de OpenLDAP como servidor de autenticación

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

72.1. Introducción.

Por favor, leer el documento titulado «Introducción a OpenLDAP.»

72.2. Equipamiento lógico necesario.

- openldap-clients-2.x
- openldap-servers-2.x
- authconfig
- authconfig-gtk (opcional)
- migrationtools

Instalación a través de yum.

Si utiliza **CentOS 6** o **Red Hat™ Enterprise Linux 6**, ejecute lo siguiente para instalar o actualizar, el equipamiento lógico necesario:

```
yum -y install openldap openldap-clients openldap-servers \
    nss-pam-ldapd authconfig authconfig-gtk \
    migrationtools
```

Nota.

Si utiliza **CentOS 5** o **Red Hat™ Enterprise Linux 5**, ejecute lo siguiente para instalar o actualizar el equipamiento lógico necesario:

```
yum -y install openldap openldap-clients openldap-servers \
    nss_ldap authconfig authconfig-gtk
```

72.3. Procedimientos.

72.3.1. SELinux y el servicio ldap.

El servicio **slapd** funcionará perfectamente con SELinux activo en modo de *imposición* (**enforcing**).

Todo el contenido del directorio **/var/lib/ldap** debe tener contexto tipo **slapd_db_t**.

```
chcon -R -t slapd_db_t /var/lib/ldap
```

Lo anterior solo será necesario si se restaura un respaldo hecho a partir de un sistema sin SELinux.

72.3.2. Certificados para TLS/SSL.

Es muy importante utilizar TLS/SSL cuando se configura el sistema para fungir como servidor de autenticación, por lo cual el siguiente procedimiento es obligatorio.

Genere el directorio **/etc/openldap/cacerts**:

```
mkdir -p /etc/openldap/cacerts
```

Cambie al directorio **/etc/openldap/cacerts**:

```
cd /etc/openldap/cacerts
```

OpenLDAP requiere primero genera una nueva autoridad certificadora. Ejecute lo siguiente:

```
echo "01" > ca.srl

openssl genrsa -aes128 2048 > cacert.key

openssl req -utf8 -new -key cacert.key -out cacert.csr

openssl x509 -req -in cacert.csr -out cacert.pem \
    -signkey cacert.key -days 3650
```

De este juego de archivos se debe compartir **cacert.pem** con todos los clientes LDAP que se conectarán al servidor. Copie este archivo dentro del directorio raíz del servidor HTTP o FTP y configure los permisos de acceso para que sea accesible desde estos servicios.

```
cp cacert.pem /var/www/html/
chmod 644 /var/www/html/cacert.pem
```

A continuación genere el certificado y firma digital para el servidor. Cabe señalar que la forma digital que será utilizada por OpenLDAP será una tipo RSA sin contraseña en formato PEM generada a partir de una firma digital con contraseña. Ejecute lo siguiente:

```
openssl genrsa -aes128 2048 > key.pem

openssl req -utf8 -new -key key.pem -out slapd.csr

openssl x509 -req -in slapd.csr -out cert.pem \
    -CA cacert.pem -CAkey cacert.key -days 3650

openssl rsa -in key.pem -out key.pem
```

Configure todos los permisos necesarios para que sólo root y el grupo ldap puedan hacer uso de los certificados y firma digital. Ejecute lo siguiente

```
cacertdir_rehash /etc/openldap/cacerts
```

Genere los enlaces necesarios para el directorio **/etc/openldap/cacerts**:

```
chown -R root:ldap /etc/openldap/cacerts
chmod -R u=rwX,g=rX,o= /etc/openldap/cacerts
```

Edite el archivo **/etc/sysconfig/ldap**:

```
vi /etc/sysconfig/ldap
```

Alrededor de la línea 20, localice #SLAPD_LDAPS=no:

```
#SLAPD_LDAPS=no
```

Elimine la almohadilla (#) y cambie no por yes, de modo que quede como **SLAPD_LDAPS=yes**.

```
SLAPD_LDAPS=yes
```

72.3.3. Creación de directorios.

Con fines de organización se creará un directorio específico para este directorio y se configurará con permisos de acceso exclusivamente al usuario y grupo ldap.

```
mkdir /var/lib/ldap/autenticar
chmod 700 /var/lib/ldap/autenticar
```

Se requiere copiar el archivo **DB_CONFIG.example** dentro del directorio **/var/lib/ldap/autenticar/**, como el archivo **DB_CONFIG**. Es decir, ejecute lo siguiente:

```
cp /usr/share/openldap-servers/DB_CONFIG.example \
    /var/lib/ldap/autenticar/DB_CONFIG
```

Nota.

Si utiliza **CentOS 5** o **Red Hat Enterprise Linux 5**, ejecute lo siguiente:

```
cp /etc/openldap/DB_CONFIG.example \
     /var/lib/ldap/autenticar/DB_CONFIG
```

Todo el contenido del directorio **/var/lib/ldap/autenticar** debe pertenecer al usuario y grupo **ldap**. Ejecute lo siguiente:

```
chown -R ldap:ldap /var/lib/ldap/autenticar
```

72.3.4. Creación de claves de acceso para LDAP.

Para crear la clave de acceso que se asignará en LDAP para el usuario administrador del directorio, ejecute lo siguiente:

```
slappasswd
```

Lo anterior debe devolver como salida un criptograma, similar al mostrado a continuación:

```
{SSHA}LnmZLFeE1/zebp7AyEF09NlGaT1d4ckz
```

Copie y respalde este criptograma. El texto de la salida será utilizado más adelante en el archivo **/etc/openldap/slapd.conf** y se definirá como clave de acceso para el usuario *Manager*, quien tendrá todos los privilegios sobre el directorio.

72.3.5. Archivo de configuración /etc/openldap/slapd.conf.

Se debe crear **/etc/openldap/slapd.conf** como archivo nuevo:

```
touch /etc/openldap/slapd.conf
vim /etc/openldap/slapd.conf
```

Nota.

Si utiliza **CentOS 5** o **Red Hat Enterprise Linux 5**, el archivo **/etc/openldap/slapd.conf** ya existe, e incluye contenido de ejemplo. Puede reemplazar todo el contenido en su totalidad, por el ejemplificado a continuación.

El archivo **/etc/openldap/slapd.conf** debe de tener definidos todos los archivos de esquema mínimos requeridos. De tal modo, el inicio del archivo debe contener algo similar a lo siguiente:

```
include         /etc/openldap/schema/corba.schema
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/duaconf.schema
include         /etc/openldap/schema/dyngroup.schema
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/java.schema
include         /etc/openldap/schema/misc.schema
include         /etc/openldap/schema/nis.schema
include         /etc/openldap/schema/openldap.schema
include         /etc/openldap/schema/ppolicy.schema
include         /etc/openldap/schema/collective.schema
include         /etc/openldap/schema/pmi.schema
```

Se deben habilitar las opciones **TLSCACertificateFile**, **TLSCertificateFile** y **TLSCertificateKeyFile** estableciendo como valores de éstas las rutas hacia el certificados y firma digital.

```
TLSCACertificateFile /etc/openldap/cacerts/cacert.pem
TLSCertificateFile /etc/openldap/cacerts/cert.pem
TLSCertificateKeyFile /etc/openldap/cacerts/key.pem
```

A fin de permitir conexiones desde clientes con OpenLDAP 2.x, establecer el archivo de número de proceso y el archivo de argumentos de LDAP, deben estar presentes las siguientes opciones, con los correspondientes valores:

```
allow bind_v2
pidfile         /var/run/openldap/slapd.pid
argsfile        /var/run/openldap/slapd.args
```

Para concluir con el **/etc/openldap/slapd.conf**, se añade lo siguiente, que tiene como finalidad el definir la configuración del nuevo directorio que en adelante se utilizará para autenticar a toda la red de área local:

```
database        bdb
suffix          "dc=dominio,dc=tld"
rootdn          "cn=Manager,dc=dominio,dc=tld"
rootpw          {SSHA}LnmZLFeE1/zebp7AyEF09NlGaT1d4ckz
directory       /var/lib/ldap/autenticar

# Indices a mantener para esta base de datos
index objectClass                       eq,pres
index ou,cn,mail,surname,givenname      eq,pres,sub
index uidNumber,gidNumber,loginShell    eq,pres
index uid,memberUid                     eq,pres,sub
index nisMapName,nisMapEntry            eq,pres,sub
```

En resumen, el archivo **/etc/openldap/slapd.conf** debiera quedar de modo similar al siguiente:

```
include         /etc/openldap/schema/corba.schema
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/duaconf.schema
include         /etc/openldap/schema/dyngroup.schema
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/java.schema
include         /etc/openldap/schema/misc.schema
include         /etc/openldap/schema/nis.schema
include         /etc/openldap/schema/openldap.schema
include         /etc/openldap/schema/ppolicy.schema
include         /etc/openldap/schema/collective.schema
include         /etc/openldap/schema/pmi.schema

TLSCACertificateFile /etc/openldap/cacerts/cacert.pem
TLSCertificateFile /etc/openldap/cacerts/cert.pem
TLSCertificateKeyFile /etc/openldap/cacerts/key.pem

allow bind_v2
pidfile         /var/run/openldap/slapd.pid
argsfile        /var/run/openldap/slapd.args

database        bdb
suffix          "dc=dominio,dc=tld"
rootdn          "cn=Manager,dc=dominio,dc=tld"
rootpw          {SSHA}LnmZLFeE1/zebp7AyEF09NlGaT1d4ckz
directory       /var/lib/ldap/autenticar

# Indices a mantener para esta base de datos
index objectClass                       eq,pres
index ou,cn,mail,surname,givenname      eq,pres,sub
index uidNumber,gidNumber,loginShell    eq,pres
index uid,memberUid                     eq,pres,sub
index nisMapName,nisMapEntry            eq,pres,sub
```

Por seguridad, el archivo **/etc/openldap/slapd.conf** deberá tener permisos de **lectura y escritura**, sólo para el usuario **ldap**.

```
chown ldap:ldap /etc/openldap/slapd.conf
chmod 600 /etc/openldap/slapd.conf
```

Nota.

Si utiliza **CentOS 5** o **Red Hat Enterprise Linux 5** o bien versiones de openldap anteriores a la 2.4, omita los siguientes tres pasos.

Elimine el conjunto de archivos y directorios que componen los configuración predeterminada:

```
rm -rf /etc/openldap/slapd.d/*
```

Es necesario crear los archivos base para el contenido del directorio **/var/lib/ldap/autenticar**, por tanto ejecute lo siguiente:

```
echo "" | slapadd -f /etc/openldap/slapd.conf
```

Convierta el archivo **/etc/openldap/slapd.conf** en el nuevo subconjunto de archivos ldif que irán dentro del directorio **/etc/ldap/slapd.d**:

```
slaptest -f \
    /etc/openldap/slapd.conf -F \
    /etc/openldap/slapd.d
```

Todo el contenido de los directorios **/etc/ldap/slapd.d** y **/var/lib/ldap/autenticar** deben pertenecer al usuario y grupo **ldap**. Ejecute lo siguiente:

```
chown -R ldap:ldap \
    /etc/openldap/slapd.d \
    /var/lib/ldap/autenticar
```

Restablezca los contextos de SELinux para los directorios **/etc/ldap/slapd.d** y **/var/lib/ldap/autenticar** ejecutando lo siguiente:

```
restorecon -R \
    /etc/openldap/slapd.d \
    /var/lib/ldap/autenticar
```

72.3.6. Inicio del servicio.

Inicie el servicio **slapd** y añada éste al resto de los servicios que arrancan junto con el sistema, ejecutando los siguientes dos mandatos:

```
service slapd start
chkconfig slapd on
```

Nota.

Si utiliza **CentOS 5** o **Red Hat Enterprise Linux 5**, inicie el servicio **slapd** y añada éste al resto de los servicios que arrancan junto con el sistema:

```
service ldap start
chkconfig ldap on
```

72.3.7. Migración de cuentas existentes en el sistema.

Edite el archivo **/usr/share/migrationtools/migrate_common.ph**:

```
vim /usr/share/migrationtools/migrate_common.ph
```

Nota.
Si utiliza **CentOS 5** o **Red Hat Enterprise Linux 5**, edite el archivo **/usr/share/openldap/migration/migrate_common.ph**:

```
vim /usr/share/openldap/migration/migrate_common.ph
```

Modifique los los valores de las variables **$DEFAULT_MAIL_DOMAIN** y `$DEFAULT_BASE` a fin de que queden del siguiente modo:

```
# Default DNS domain
$DEFAULT_MAIL_DOMAIN = "dominio.tld";

# Default base
$DEFAULT_BASE = "dc=dominio,dc=tld";
```

A continuación, hay que crear el objeto que a su vez contendrá el resto de los datos en el directorio, utilizando **migrate_base.pl** para generar el archivo **base.ldif**.

Genere el archivo **base.ldif**, ejecutando lo siguiente:

```
/usr/share/migrationtools/migrate_base.pl > base.ldif
```

Nota.
Si utiliza **CentOS 5** o **Red Hat Enterprise Linux 5**, puede generar el archivo base.ldif ejecutando lo siguiente:

```
/usr/share/openldap/migration/migrate_base.pl > base.ldif
```

Utilice el mandato **ldapadd** para insertar los datos necesarios. Las opciones utilizadas con este mandato son las siguientes:

```
-x              autenticación simple
-W              solicitar clave de acceso
-D binddn       Nombre Distinguido (dn) a utilizar
-h anfitrión    Servidor LDAP a acceder
-f archivo      archivo a utilizar
```

Una vez entendido lo anterior, se procede a insertar la información generada en el directorio utilizando lo siguiente:

```
ldapadd -x -W -D 'cn=Manager,dc=dominio,dc=tld' \
    -h 127.0.0.1 -f base.ldif
```

Una vez hecho lo anterior, se podrá comenzar a poblar el directorio con datos. Lo primero será importar los grupos y usuarios existentes en el sistema. Realice la importación de usuarios creando los archivos **group.ldif** y **passwd.ldif**, utilizando **migrate_group.pl** y **migrate_passwd.pl**.

Ejecute los siguientes dos mandatos:

```
/usr/share/migrationtools/migrate_group.pl \
    /etc/group group.ldif
/usr/share/migrationtools/migrate_passwd.pl \
    /etc/passwd passwd.ldif
```

Nota.

Si utiliza **CentOS 5** o **Red Hat Enterprise Linux 5**, ejecute los siguientes dos mandatos:

```
/usr/share/openldap/migration/migrate_group.pl \
    /etc/group group.ldif
/usr/share/openldap/migration/migrate_passwd.pl \
    /etc/passwd passwd.ldif
```

Lo anterior creará los archivos **group.ldif** y **passwd.ldif**, los cuales incluirán la información de los grupos y cuentas en el sistema, incluyendo las claves de acceso. Los datos se podrán insertar en el directorio LDAP utilizando lo siguiente:

```
ldapadd -x -W -D 'cn=Manager,dc=dominio,dc=tld' \
    -h 127.0.0.1 -f group.ldif
ldapadd -x -W -D 'cn=Manager,dc=dominio,dc=tld' \
    -h 127.0.0.1 -f passwd.ldif
```

72.4. Comprobaciones.

Antes de configurar el sistema para utilizar LDAP para autenticar, es conveniente verificar que todo funciona correctamente.

El siguiente mandato verifica que directorios disponibles existen en el servidor 127.0.0.1.

```
ldapsearch -h 127.0.0.1 -x -b '' -s base \
    '(objectclass=*)' namingContexts
```

Lo anterior debe devolver una salida similar a lo siguiente:

```
# extended LDIF
#
# LDAPv3
# base <> with scope base
# filter: (objectclass=*)
# requesting: namingContexts
#

#
dn:
namingContexts: dc=dominio,dc=tld

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

El siguiente mandato debe devolver toda la información de todo el directorio solicitado (**dc=dominio**,**dc=tld**).

```
ldapsearch -x -b 'dc=dominio,dc=tld' '(objectclass=*)'
```

Otro ejemplo es realizar una búsqueda específica, para un usuario en particular. Asumiendo que en el directorio existe el usuario denominado *fulano*, ejecute lo siguiente:

```
ldapsearch -x -b 'uid=fulano,ou=People,dc=dominio,dc=tld'
```

Lo anterior debe regresar algo similar a lo siguiente:

```
# extended LDIF
#
# LDAPv3
# base uid=fulano,ou=People,dc=dominio,dc=tld with scope sub
# filter: (objectclass=*)
# requesting: ALL
#

# fulano, People, dominio.tld
dn: uid=fulano,ou=People,dc=dominio,dc=tld
uid: fulano
cn: fulano
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword:: xxxxxxxxxxxx
shadowLastChange: 12594
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 505
gidNumber: 505
homeDirectory: /home/fulano

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

72.5. Configuración de clientes.

Los clientes **CentOS 6** y **Red Hat Enterprise Linux 6**, requieren tener instalados los paquetes **nss-pam-ldap**, authconfig y **openldap-clients-2.4.23-16.el6** (las versiones anteriores de este último tienen roto el soporte para TLS/SSL):

```
yum -y install authconfig openldap-clients nss-pam-ldapd
```

Nota.

Los clientes **CentOS 5** y **Red Hat Enterprise Linux 5** requieren tener instalados los paquetes **nss_ldap**, authconfig y openldap-clients:

```
yum -y install authconfig openldap-clients nss_ldap
```

Defina los valores para las opciones **host** y **base**, a fin de establecer hacia que servidor y a que directorio conectarse, en el archivo **/etc/pam_ldap.conf**.

```
vim /etc/pam_ldap.conf
```

Nota.
Si utiliza **CentOS 5** o **Red Hat™ Enterprise Linux 5**, defina lo anterior en el archivo **/etc/ldap.conf**.

```
vim /etc/ldap.conf
```

Para fines prácticos, el valor de la opción **uri** corresponde al nombre del servidor LDAP, previamente resuelto por un DNS y el valor de la opción **base** debe ser el mismo que se especificó en el archivo **/etc/openldap/slapd.conf** para la opción **suffix**. Considerando que el nombre de anfitrión del servidor LDAP está resuelto por un servidor DNS, como **servidor.dominio.tld**, puede definir lo siguiente:

```
uri ldap://servidor.dominio.tld/
base dc=dominio,dc=tld
ssl start_tls
tls_checkpeer no
pam_password md5
```

Asumiendo que el servidor LDAP tiene definido como nombre de anfitrión **servidor.dominio.tld**, previamente resuelto en un servidor DNS, ejecute lo siguiente:

```
authconfig --useshadow  --passalgo=sha512 --enablelocauthorize \
    --enablemkhomedir --enableldap --enableldapauth \
    --ldapserver=servidor.dominio.tld \
    --ldapbasedn=dc=dominio,dc=tld --enableldaptls \
    --ldaploadcacert=http://servidor.red-local.net/cacert.pem \
    --update
```

Al terminar, debe iniciar y agregar a los servicios de arranque del sistema al servicio **nslcd**.

```
chkconfig nslcd on
service nslcd start
```

72.6. Administración.

Existen muchos programas para acceder y administrar servidores LDAP, pero la mayoría sólo sirven para administrar usuarios y grupos del sistema, como el módulo de LDAP de Webmin. La herramienta de administración de directorios LDAP más sencilla de utilizar pudiera ser PHP LDAP Admin.

72.7. Respaldo de datos.

El procedimiento requiere detener el servicio **slapd**.

```
service slapd stop
```

Nota.
Si utiliza **CentOS 5** o **Red Hat Enterprise Linux 5**, debe detenerse el servicio **ldap** antes de proceder con el respaldo de datos.

```
service ldap stop
```

Utilice el mandato **slapcat** del siguiente modo, definiendo el directorio de configuración **/etc/openldap/slapd.d**.

```
slapcat -v -F /etc/openldap/slapd.d \
    -l respaldo-$(date +%Y%m%d).ldif
```

Nota.
Si utiliza **CentOS 5** o **Red Hat Enterprise Linux 5**, se utiliza la herramienta **slapcat**, definiendo el archivo de configuración **/etc/openldap/slapd.conf**.

```
slapcat -v -f /etc/openldap/slapd.conf \
    -l respaldo-$(date +%Y%m%d).ldif
```

Inicie de nuevo el servicio **slapd**.

```
service slapd start
```

Nota.
Si utiliza **CentOS 5** o **Red Hat Enterprise Linux 5**, inicie de nuevo el servicio **ldap**.

```
service ldap start
```

72.8. Restauración de datos.

El procedimiento requiere detener el servicio. Ejecute lo siguiente:

```
service slapd stop
```

Nota.
Si utiliza **CentOS 5** o **Red Hat Enterprise Linux 5**, ejecute lo siguiente:

```
service ldap stop
```

Deben eliminarse los datos del directorio a restaurar.

```
rm -f /var/lib/ldap/autenticar/*
```

Vuelva a copiar el archivo **DB_CONFIG.example** dentro del directorio **/var/lib/ldap/autenticar/**, como el archivo **DB_CONFIG**. Es decir, ejecute lo siguiente:

```
cp /usr/share/openldap-servers/DB_CONFIG.example \
    /var/lib/ldap/autenticar/DB_CONFIG
```

Utilice la herramienta **slapadd** para cargar los datos del respaldo desde un archivo *.ldif.

```
slapadd -v -c \
    -l respaldo-20110911.ldif \
    -F /etc/openldap/slapd.d
```

Nota.

Si utiliza **CentOS 5** o **Red Hat Enterprise Linux 5**, **slapadd** se utiliza definiendo el archivo de configuración **/etc/openldap/slapd.conf**.

```
slapadd -v -c \
    -l respaldo-20110911.ldif \
    -f /etc/openldap/slapd.conf
```

Para regenerar los índices LDAP, ejecute el mandato **slapindex**:

```
slapindex
```

Inicie de nuevo el servicio, ejecutando lo siguiente:

```
service slapd start
```

Nota.

Si utiliza **CentOS 5** o **Red Hat Enterprise Linux 5**, ejecute lo siguiente:

```
service ldap start
```

72.9. Modificaciones necesarias en el muro cortafuegos.

Es necesario abrir los puertos 389/TCP (**ldap**) y 636/TCP (**ldaps**).

72.9.1. Servicio iptables.

Ejecute lo siguiente para anexar las reglas de **iptables** correspondientes:

```
iptables -A INPUT -m state \
    --state NEW -m tcp -p tcp \
    --dport 389 -j ACCEPT
iptables -A INPUT -m state \
    --state NEW -m tcp -p tcp \
    --dport 636 -j ACCEPT
```

Ejecute lo siguiente para guardar los cambios:

```
service iptables save
```

O bien añada lo siguiente al archivo **/etc/sysconfig/iptables**:

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 389 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 636 -j ACCEPT
```

Y reinicie el servicio **iptables**:

```
service iptables restart
```

72.9.2. Shorewall.

Si utiliza **Shorewall**, edite el archivo **/etc/shorewall/rules**:

```
vim /etc/shorewall/rules
```

Las reglas corresponderían a algo similar a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  net     fw      tcp     389,636
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Al terminar de configurar las reglas para **Shorewall**, reinicie el muro cortafuegos, ejecutando el siguiente mandato:

```
service shorewall restart
```

73. Configuración básica de MySQL™.

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

73.1. Introducción.

73.1.1. Acerca de MySQL™.

MySQL™ es un **DBMS** (**D**ata**B**ase **M**anagement **S**ystem) o sistema de gestión de base de datos **SQL** (**S**tructured **Q**uery **L**anguage o Lenguaje Estructurado de Consulta) multiusuario y multihilo con licencia **GNU/GPL**. Fue propiedad y patrocinio de **MySQL AB**, compañía fundada por David Axmark, Allan Larsson y Michael Widenius, con base de operaciones en Suecia, la cual poseía los derechos de autor de prácticamente todo el código que lo integraba. **MySQL AB** desarrolló y se encargó del mantenimiento de MySQL vendiendo servicios de soporte y otros valores agregados, así como también licenciamiento privativos para los desarrollos de equipamiento lógico que requieren mantener cerrado su código fuente. MySQL™ AB fue adquirido en 2008 por Sun Microsystems, que a su vez fue adquirido por Oracle Corporation en 2009.

MySQL™ es actualmente el servidor de base de datos más popular para los desarrollos a través de la red mundial, principalmente sitios de Internet. Es célebre y casi legendario, por considerarse rápido y sólido. MySQL será reemplazado de forma transparente por MariaDB, una bifurcación de MySQL dirigida por Michael Widenius, como medida para hacer frente a la mala gestión que ha realizado Oracle sobre el proyecto MySQL.

URL: http://www.mysql.com/

73.2. Equipamiento lógico necesario.

73.2.1. En CentOS, Fedora™ y Red Hat™ Enterprise Linux.

Ejecute lo siguiente para instalar los paquetes mysql (cliente) y mysql-server (servidor):

```
yum -y install mysql mysql-server
```

73.2.2. En openSUSE™ y SUSE™ Linux Enterprise.

Ejecute lo siguiente para instalar los paquetes mysql-client (cliente) y mysql (servidor):

```
yast -i mysql mysql-client
```

73.3. Modificaciones necesarias en el muro cortafuegos.

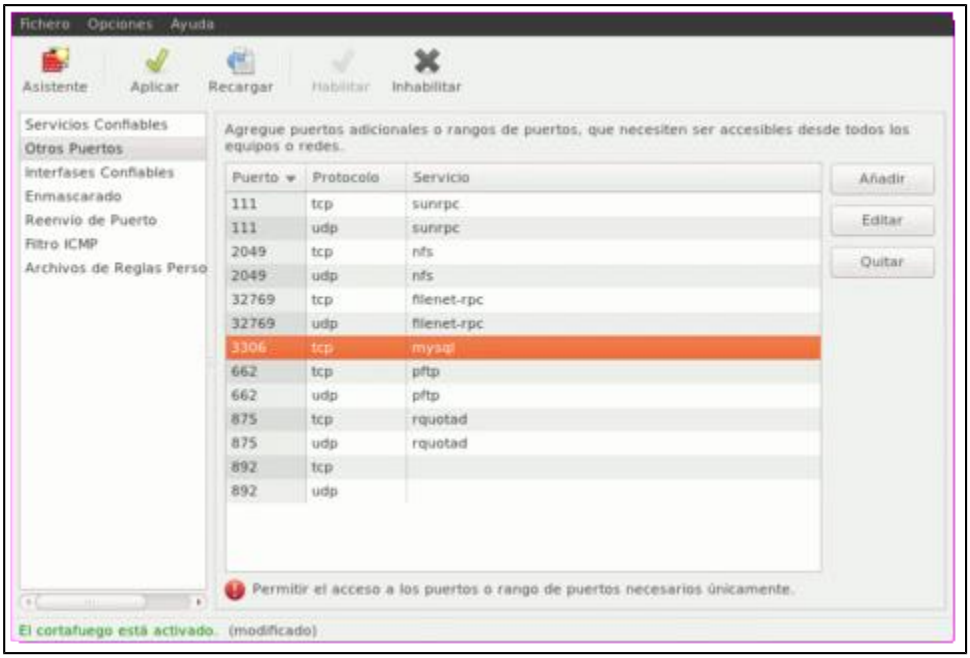
Es necesario abrir el puerto 3306 por TCP (**mysql**), pero sólo si requiere hacer conexiones desde anfitriones remotos.

73.3.0.1. Herramienta system-config-firewall.

Si utiliza el muro cortafuegos predeterminado del sistema, puede ejecutar el siguiente mandato:

```
system-config-firewall
```

Habilite el puertos **3306/TCP** y aplique los cambios.



Herramienta system-config-firewall habilitando el puerto 3306/TCP pata MySQL.

73.3.0.2. Servicio iptables.

Si lo prefiere, también puede utilizar directamente el mandato **iptables**, ejecutando lo siguiente:

```
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 3306 -j ACCEPT
service iptables save
```

O bien añada lo siguiente al archivo **/etc/sysconfig/iptables**:

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 3306 -j ACCEPT
```

Y reinicie el servicio **iptables**:

```
service iptables restart
```

73.3.0.3. Shorewall.

La regla para el archivo **/etc/shorewall/rules** de **Shorewall** correspondería a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  all     fw      tcp     3306
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Para aplicar los cambios en Shorewall, ejecute lo siguiente:

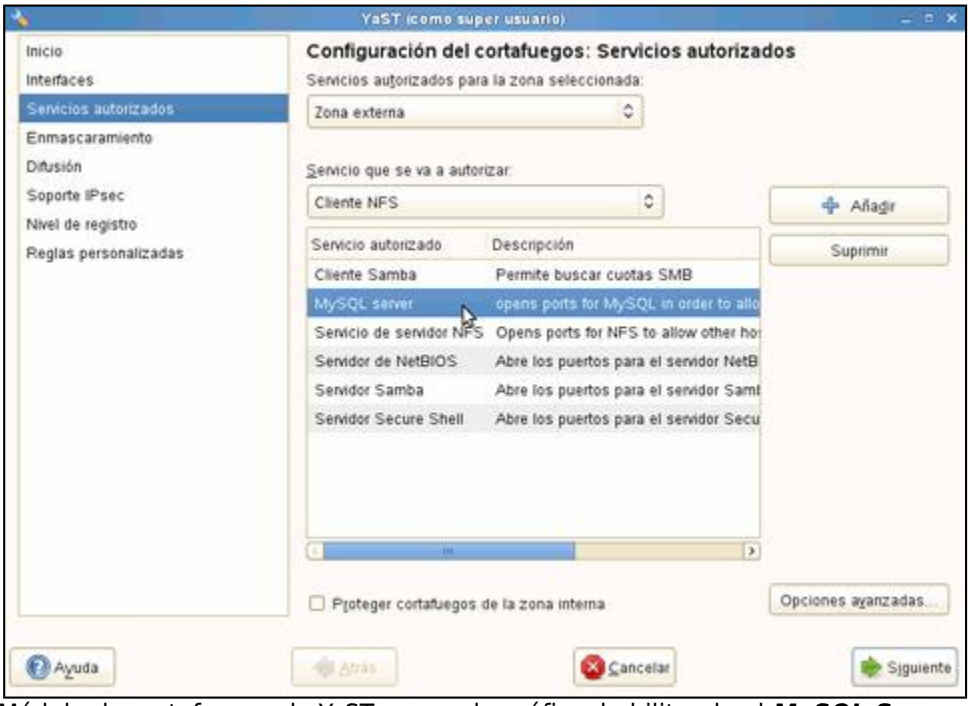
```
service shorewall restart
```

73.3.1. En openSUSE™ y SUSE™ Linux Enterprise.

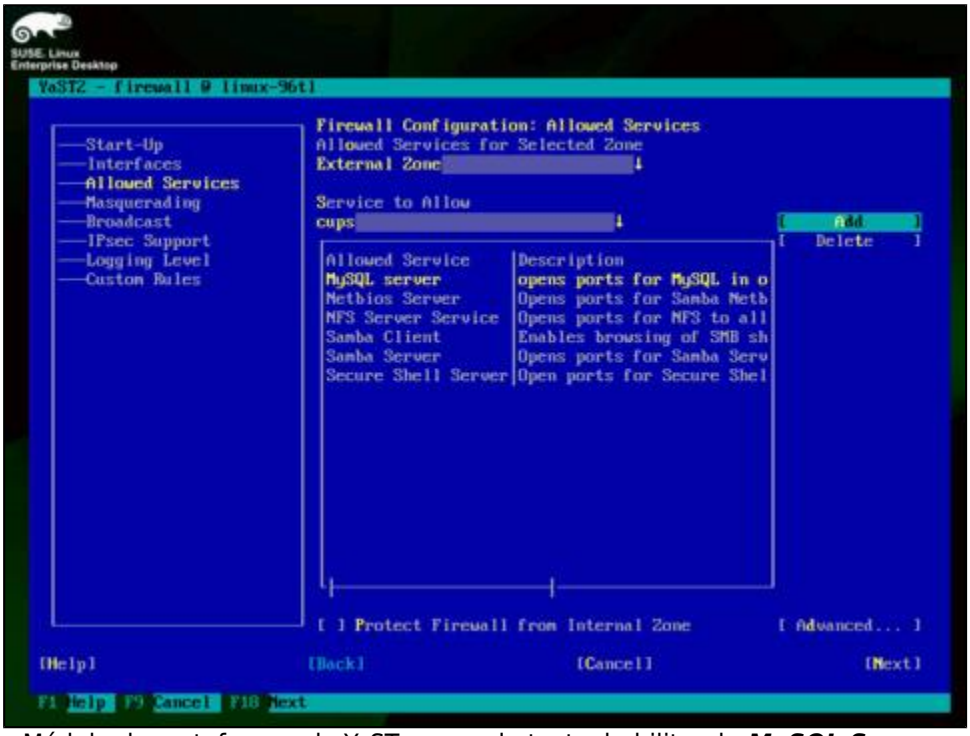
Ejecute el mandato **yast** del siguiente modo:

```
yast firewall
```

Y habilite ***MySQL Server*** y aplique los cambios. Ésto habilitará todos los puertos necesarios.



Módulo de cortafuegos de YaST, en modo gráfico, habilitando el ***MySQL Server***.



Módulo de cortafuegos de YaST, en modo texto, habilitando ***MySQL Server***.

73.4. SELinux y MySQL™, sólo en CentOS, Fedora™ y Red Hat™ Enterprise Linux.

Para que SELinux permita al usuario regular establecer conexiones hacia el zócalo de MySQL™, utilice el siguiente mandato:

```
setsebool -P allow_user_mysql_connect 1
```

Para que SELinux permita al servicio **mysqld** conectarse a cualquier puerto distinto al 3306, utilice el siguiente mandato:

```
setsebool -P mysql_connect_any 1
```

73.5. Procedimientos.

73.5.1. Iniciar, detener y reiniciar el servicio mysqld.

73.5.1.1. En CentOS, Fedora™ y Red Hat™ Enterprise Linux.

Para que el servicio de **mysqld** esté activo en todos los niveles de ejecución, se ejecuta lo siguiente:

```
chkconfig mysqld on
```

Para iniciar por primera vez el servicio **mysqld** y generar la base de datos inicial (**mysql**), ejecute lo siguiente:

```
service mysqld start
```

Para reiniciar el servicio **mysqld**, ejecute lo siguiente:

```
service mysqld restart
```

Para detener el servicio **mysqld**, ejecute lo siguiente:

```
service mysqld stop
```

73.5.1.2. openSUSE™ y SUSE™ Linux Enterprise.

Para que el servicio de **mysql** esté activo en todos los niveles de ejecución, se ejecuta lo siguiente:

```
insserv mysql
```

Para iniciar por primera vez el servicio **mysql** y generar la base de datos inicial (**mysql**), ejecute lo siguiente:

```
rcmysql start
```

Para reiniciar el servicio **mysql**, ejecute lo siguiente:

```
rcmysql restart
```

Para detener el servicio **mysql**, ejecute lo siguiente:

```
rcmysql stop
```

73.5.2. Archivos y directorios de configuración.

El archivo **/etc/my.cnf** es el utilizado para establecer o cambiar opciones permanentes de MySQL. Las bases de datos se almacenan dentro del directorio **/var/lib/mysql**.

73.5.3. Asignación de contraseña al usuario root en MySQL.

El usuario **root** en MySQL™, carece de contraseña después de iniciado el servicio por primera vez, por lo cual es muy importante asignar una.

Si necesita poner en producción inmediatamente el servidor, ejecute el mandato **mysql_secure_installation** para iniciar un asistente que le permitirá asignar una contraseña al usuario root de MySQL, eliminar el usuario anónimo y la base de dato de pruebas (test), eliminar accesos remoto y otros ajustes de seguridad importantes.

```
mysql_secure_installation
```

Con lo anterior, recuerde que inicialmente el usuario root carece de contraseña. Cuando se le solicite asignar la contraseña de root se le solcitará la contraseña actual. Sólo pulse la tecla ENTER y luego asigne una nueva contraseña.

En adelante, será necesario añadir la opción **-p** a cualquier sentencia de línea de mandatos para **mysql**, **mysqladmin** y **mysqldump** para ingresar la contraseña del usuario **root** y poder, de esta forma, realizar diversas tareas administrativas.

De manera alternativa, puede ejecutar el mandato **mysqladmin**, con la opción **-h** con **localhost** como argumento, la opción **-u** con **root** y **password** como argumentos y la nueva contraseña entre comillas simples:

```
mysqladmin -u root password 'cualquier-contraseña-que-guste'
```

73.5.3.1. Recuperación de la contraseña del usuario root en MySQL.

En caso de que haya olvidado la contraseña del usuario **root** de MySQL™, detenga el servicio ejecutando **service mysqld stop** (CentOS, Fedora™ y Red Hat™ Enterprise Linux) o bien **rcmysql stop** (openSUSE™ y SUSE™ Linux Enterprise).

Ejecute el mandato **mysqld_safe** con la opción **--skip-grant-tables**, enviando el proceso a segundo plano:

```
mysqld_safe --skip-grant-tables &
```

Ingrese al intérprete de mandato de MySQL™ ejecutando el mandato **mysql**, sin argumentos u opciones:

```
mysql
```

Ejecute lo siguiente:

```
UPDATE mysql.user
SET Password=PASSWORD('nueva-contraseña')
WHERE User='root';
FLUSH PRIVILEGES;
```

Salga del intérprete de mandatos de MySQL™ ejecutando lo siguiente:

```
exit;
```

Detenga el servicio **mysqld** ejecutando sólo lo siguiente:

```
mysqladmin shutdown
```

Inicie MySQL™ ejecutando **service mysqld start** (CentOS, Fedora™ y Red Hat™ Enterprise Linux) o bien **rcmysql start** (openSUSE™ y SUSE™ Linux Enterprise).

Verifique el cambio de contraseña accediendo a MySQL™ con el mandato **mysql** y la opción **-p**, e ingrese la nueva contraseña.

```
mysql -p
```

Salga del intérprete de mandatos de MySQL™ ejecutando lo siguiente:

```
exit;
```

Procure memorizar la nueva contraseña asignada al usuario root de MySQL.

73.5.4. Crear y eliminar bases de datos.

Para crear una nueva base de datos, puede utilizarse el mandato **mysqladmin** con el parámetro **create**, la opción **-u** con root como usuario y la opción **-p** para indicar que se ingresará una contraseña:

```
mysqladmin -u root -p create basedatos
```

Para eliminar una base de datos, se utiliza el mandato **mysqladmin** con el parámetro **drop** en lugar de **create**, la opción **-u** con root como usuario y la opción **-p** para indicar que se ingresará una contraseña:

```
mysqladmin -u root -p drop basedatos
```

73.5.5. Respaldo y restauración de bases de datos.

Para respaldar una base de datos desde el anfitrión local, se ejecuta el mandato **mysqldump** con las opciones **--opt** (que añade automáticamente las opciones --add-drop-table, --add-locks, --create-options, --quick, --extended-insert, --lock-tables, --set-charset y --disable-keys), la opción **-u** con el nombre de usuario a utilizar, la opción **-p** para indicar que se ingresará una contraseña, el nombre de la base de datos, **>** para guardar la salida estándar (STDOUT) en un archivo y el nombre del archivo donde se guardará el respaldo. Ejemplo:

```
mysqldump --opt -u root -p basedatos > respaldo.sql
```

Para restaurar un respaldo, se ejecuta el mandato **mysql** con las opciones **-u** con el nombre de usuario con privilegios sobre la base de datos a restaurar, **-p** para indicar que se utilizará contraseña, el nombre de la base de datos a restaurar, **<** para indicar que la entrada estándar (**STDIN**) será un archivo y el nombre del archivo con el respaldo de la base de datos. Ejemplo:

```
mysql -u root -p basedatos < respaldo.sql
```

Para respaldar todas la bases de datos hospedadas en MySQL™, se ejecuta el mandato **mysqldump** con las opciones **--opt**, **--all-databases** para indicar que se respaldarán todas la bases de datos, la opción **-u** con root como usuario, la opción **-p** para indicar que se utilizará contraseña, el símbolo **>** para guardar la salida estándar (**STDOUT**) en un archivo y el nombre del archivo donde se guardará el respaldo. Ejemplo:

```
mysqldump --opt --all-databases -u root -p > respaldo-todo.sql
```

Para restaurar todas las bases de datos a partir de un único archivo de respaldo, se ejecuta el mandato **mysql** con la opción **-u** con root como usuario, la opción **-p** para indicar que se utilizará contraseña, el símbolo **<** para indicar que la entrada estándar (**STDIN**) será un archivo y el nombre del archivo con el respaldo de todas las bases de datos. Ejemplo:

```
mysql -u root -p < respaldo-todo.sql
```

73.5.6. Permisos de acceso a las bases de datos.

Ingrese al intérprete de MySQL™ como el usuario **root**:

```
mysql -u root -p
```

Para asignar los permisos **select** (seleccionar), **insert** (insertar), **update** (actualizar), **create** (crear), **alter** (alterar), **delete** (eliminar) y **drop** (descartar) sobre las tablas de una base de datos al usuario **prueba** desde el anfitrión **localhost** (anfitrión local), se ejecuta algo similar a lo siguiente:

```
GRANT
 select, insert, update, create, alter, delete, drop
ON
 base-de-datos.*
TO
 usuario@localhost
IDENTIFIED BY
 'contraseña';
```

Puede otorgar al usuario todos los permisos sobre la base de datos ejecutando lo siguiente:

```
GRANT
 all
ON
 base-de-datos.*
TO
 usuario@localhost
IDENTIFIED BY
 'contraseña';
```

Si se requiere permitir el acceso hacia una base de datos desde otro anfitrión en la red de área local, se ejecuta algo similar al ejemplo anterior, pero definiendo el usuario y la dirección IP del anfitrión remoto. Ejemplo:

```
GRANT
 select, insert, update, create, alter, delete, drop
ON
 directorio.*
TO
 usuario@192.168.70.2
IDENTIFIED BY
 'contraseña';
```

Puede otorgar al usuario todos los permisos sobre la base de datos ejecutando lo siguiente:

```
GRANT
 all
ON
 directorio.*
TO
 usuario@192.168.70.2
IDENTIFIED BY
 'contraseña';
```

Si se requiere permitir el acceso hacia una base de datos desde cualquier anfitrión, se ejecuta algo similar a lo anterior, pero definiendo el nombre del usuario entre comillas simples, arroba y el símbolo % entre comillas simples. Ejemplo:

```
GRANT
 all
ON
 directorio.*
TO
 'usuario'@'%'
IDENTIFIED BY
 'contraseña-usuario-usuario';
```

73.6. Optimización de MySQL.

73.6.1. Deshabilitar la resolución de nombres de anfitrión.

MySQL mantiene un cache de anfitriones utilizados en la memoria, la cual contiene las direcciones IP, nombres de anfitrión y errores de información asociados a éstos. El cache sólo se utiliza para conexiones TCP remotas con otros anfitriones y jamás lo utiliza para conexiones a través de la interfaz de retorno del sistema (loopback, 127.0.0.1) o conexiones hechas a través del archivo de zócalo, tubería o bien memoria compartida.

Por cada nueva conexión, MySQL™ utiliza la dirección IP del cliente para verificar si el nombre de anfitrión de éste está en el cache de anfitriones. Cuando el nombre es inexistente, MySQL™ intentará resolver el nombre de anfitrión, resolviendo primero la dirección IP, luego resolviendo el nombre, comparando el resultado de la dirección IP original para verificar que correspondan. MySQL™ almacena luego esta información en el cache de anfitriones.

El objetivo del cache es evitar hacer una consulta de DNS por cada conexión de cliente y el almacenamiento de información de errores que ocurren en el proceso de conexión de los clientes. Cuando ocurren demasiados errores desde un anfitrión en particular y se rebasa el valor de la variable **max_connect_errors** (10, de modo predeterminado), MySQL™ bloquea el acceso desde dicho anfitrión.

Cuando un anfitrión es bloqueado, sólo podrá acceder de nuevo si se reinicia MySQL™ o si se limpia el cache de anfitriones. Este último puede limpiarse ejecutando desde el intérprete de mandatos del sistema lo siguiente:

```
mysqladmin -p flush-hosts
```

Cuando se tiene un DNS muy lento o se carece de uno que resuelva el nombre de los anfitriones o bien se tiene demasiados anfitriones haciendo conexiones hacia el servidor MySQL™, deshabilitar el cache de anfitriones o hacer más grande éste, mejora el rendimiento considerablemente. La consecuencia de deshabilitar el cache de anfitriones es que en adelante sólo se podrán otorgar permisos de acceso y realizar conexiones utilizando direcciones IP, es decir utilizando ***usuario@a.b.c.d*** en lugar de ***usuario@anfitrión.dominio.tld***.

Para deshabilitar el cache de anfitriones, se requiere editar el archivo **/etc/my.cnf**:

```
vi /etc/my.cnf
```

Y añadir la siguiente opción en la sección **[mysqld]**:

```
skip-name-resolve
```

Para aplicar los cambios, es necesario reiniciar el servicio.

Si se desea hacer más grande el cache de anfitriones, cuyo valor predeterminado es 128 anfitriones, se requiere cambiar el valor de **HOST_CACHE_SIZE** por cualquier valor entre 0 y 2048 y compilar MySQL™ desde código fuente, motivo por el cual es más práctico deshabilitar el cache de anfitriones.

73.6.2. Aumentar el tamaño de cache de consultas.

Cuando se habilita el cache de consultas en memoria y se dispone de suficiente de ésta, el desempeño del servidor MySQL™ se incrementa considerablemente. El valor predeterminado del tamaño cache de consultas (**query_cache_size**) es 0, lo que significa que está desactivado. Los valores permitidos son múltiplos de 1024 (bytes). Si, por ejemplo, se desea establecer un tamaño de cache de consultas de **32 MiB**, el valor sería ***33882112*** bytes.

Ingrese al intérprete de MySQL™ como el usuario **root**:

```
mysql -u root -p
```

Verifique el valor de la variable **query_cache_size** ejecutando lo siguiente:

```
SHOW VARIABLES LIKE '%query_cache%';
```

La salida será similar a la siguiente:

```
+------------------------------+---------+
| Variable_name                | Value   |
+------------------------------+---------+
| have_query_cache             | YES     |
| query_cache_limit            | 1048576 |
| query_cache_min_res_unit     | 4096    |
| query_cache_size             | 0       |
| query_cache_type             | ON      |
| query_cache_wlock_invalidate | OFF     |
+------------------------------+---------+
6 rows in set (0.00 sec)
```

Ejecute lo siguiente para cambiar el valor de **query_cache_size** a ***32 MiB***:

```
SET GLOBAL query_cache_size = 33882112;
```

Verifique el cambio ejecutando lo siguiente:

```
SHOW VARIABLES LIKE '%query_cache%';
```

La salida será similar a la siguiente:

```
+------------------------------+----------+
| Variable_name                | Value    |
+------------------------------+----------+
| have_query_cache             | YES      |
| query_cache_limit            | 1048576  |
| query_cache_min_res_unit     | 4096     |
| query_cache_size             | 33882112 |
| query_cache_type             | ON       |
| query_cache_wlock_invalidate | OFF      |
+------------------------------+----------+
6 rows in set (0.00 sec)
```

Salga del intérprete de MySQL.

```
exit;
```

El cambio prevalecerá hasta que sea reiniciado MySQL. Para que el cambio sea permanente, se requiere editar el archivo **/etc/my.cnf**:

```
vi /etc/my.cnf
```

Y añadir la siguiente opción en la sección **[mysqld]**:

```
query_cache_size = 33882112
```

Para aplicar los cambios, es necesario reiniciar el servicio. Ejecute:

```
service mysqld restart
```

Para verificar el estado del cache de consultas, ingrese al intérprete de mandatos de MySQL™:

```
mysql -u root -p
```

A fin de generar algo de actividad, realice algunas consultas al azar hacia cualquier base de datos MySQL™ hospedada en el servidor. Sólo la primera consulta que haga siempre será un poco más lenta que las subsecuentes. El resto de las consultas deberán ser más rápidas.

Para verificar el estado del cache de consultas, vuelva a ingresar ingresar al intérprete de mandatos de MySQL™:

```
mysql -u root -p
```

Desde el intérprete de mandatos de MySQL™ ejecute lo siguiente:

```
SHOW STATUS LIKE '%Qcache%';
```

La salida puede ser similar a la siguiente:

```
+-------------------------+----------+
| Variable_name           | Value    |
+-------------------------+----------+
| Qcache_free_blocks      | 1        |
| Qcache_free_memory      | 33864568 |
| Qcache_hits             | 0        |
| Qcache_inserts          | 0        |
| Qcache_lowmem_prunes    | 0        |
| Qcache_not_cached       | 61       |
| Qcache_queries_in_cache | 0        |
| Qcache_total_blocks     | 1        |
+-------------------------+----------+
8 rows in set (0.00 sec)
```

73.6.3. Soporte para UTF-8.

Algunas aplicaciones, como vTigerCRM, requieren se configuré UTF-8 como codificación predeterminada de MySQL. Edite el archivo **/etc/my.cnf**:

```
vi /etc/my.cnf
```

Añada las siguientes líneas **resaltadas**:

```
[mysql]
default-character-set=utf8

[mysqld]
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
user=mysql
# Disabling symbolic-links is recommended to prevent assorted security risks
symbolic-links=0
skip-name-resolve
query_cache_size = 33882112
collation_server=utf8_unicode_ci
character-set-server=utf8
init_connect='SET collation_connection = utf8_general_ci'
init_connect='SET NAMES utf8'

[mysqld_safe]
log-error=/var/log/mysqld.log
pid-file=/var/run/mysqld/mysqld.pid
```

Al terminar, sólo es necesario reiniciar el servicio **mysqld** para que surtan efecto los cambios.

```
service mysqld restart
```

73.7. Bibliografía.

- http://dev.mysql.com/doc/refman/5.0/en/host-cache.html

74. Configuración básica de Apache.

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

74.1. Introducción.

74.1.1. Acerca del protocolo HTTP.

HTTP (***H****yper****t****ext* ***T****ransfer* ***P****rotocol* o Protocolo de Trasferencia de Hipertexto) es el método utilizado para transferir o transportar información a través de Internet y (WWW, ***W****orld* ***W****ide* ***W****eb*). Su propósito original fue el proveer una forma de publicar y recuperar documentos en formato HTML.

El desarrollo del protocolo fue coordinado por ***World Wide Web Consortium*** y la **IETF** (***I****nternet* ***E****ngineering* ***T****ask* ***F****orce* o Fuerza de Trabajo en Ingeniería de Internet), culminando con la publicación de varios RFC (***R****equest* ***F****or* ***C****omments*), de entre los que destaca el RFC 2616, mismo que define la versión 1.1 del protocolo, que es el utilizado hoy en día.

HTTP es un protocolo de solicitud y respuesta a través de **TCP**, entre agentes de usuario (Navegadores, motores de índice y otras herramientas) y servidores, regularmente utilizando el puerto 80. Entre la comunicación entre éstos puede intervenir otros tipos de implementaciones, como serían servidores Intermediarios (*Proxies), puertas de enlace y túneles.*

URL: http://tools.ietf.org/html/rfc2616

74.1.2. Acerca de Apache.

Apache es un servidor HTTP de código fuente abierto y licenciamiento libre que funciona en Linux, sistemas operativos derivados de Unix™, Windows™, Novell™ Netware y otras plataformas. Ha desempeñado un papel muy importante en el crecimiento de Internet y continua siendo el servidor HTTP más utilizado, siendo además el servidor *de facto* contra el cual se realizan las pruebas comparativas y de desempeño para otros productos competidores. Es desarrollado y mantenido por una comunidad de desarrolladores auspiciada por ***Apache Software Foundation***.

URL: http://www.apache.org/

74.2. Equipamiento lógico necesario.

74.2.1. En CentOS, Fedora™ y Red Hat™ Enterprise Linux.

Ejecute lo siguiente:

```
yum -y install httpd
```

Si se desea incluir soporte para **PHP**/**MySQL**, **Perl**, **Python** y **SSL**/**TLS**, ejecute lo siguiente:

```
yum -y install php php-mysql mod_perl mod_wsgi mod_ssl
```

Nota.

En **CentOS 6**, **Fedora™** y **Red Hat™ Enterprise Linux 6**, el soporte para Python se incluye con el paquete **mod_wsgi**. En **CentOS 5** y **Red Hat™ Enterprise Linux 5**, el soporte para Python se incluye con el paquete **mod_python**.

```
yum -y install mod_python
```

Para poder realizar pruebas desde el mismo anfitrión local, puede utilizar cualquier navegador, como serían Firefox y Google Chrome. A fin de poder prescindir del uso del modo gráfico y poder trabajar desde una terminal de texto, sugerimos instalar y utilizar el navegador Lynx.

```
yum -y install lynx
```

74.3. Iniciar servicio y añadir el servicio al arranque del sistema.

Para añadir el servicio al arranque del sistema, ejecute:

```
chkconfig httpd on
```

Para iniciar el servicio ejecute:

```
service httpd start
```

Para reiniciar el servicio interrumpiendo todas las conexiones establecidas en ese momento, ejecute:

```
service httpd restart
```

Para cargar los cambios en la configuración sin interrumpir el servicio y con ésto mantener activas las conexiones establecidas, ejecute

```
service httpd reload
```

Para detener el servicio, ejecute:

```
service httpd stop
```

74.4. SELinux y Apache.

En **CentOS**, **Fedora™** y **Red Hat™ Enterprise Linux**, de modo predeterminado SELinux viene activo en modo obligatorio (*enforcing*). Éste añade seguridad y protección adicional a Apache. Sin embargo algunas opciones impedirán utilizar ciertas funciones en Apache, como directorios virtuales fuera del directorio /var/www, directorios ~/public_html, el envío de correo electrónico desde aplicaciones basadas sobre HTTP, etc.

Para permitir a Apache poder enviar correo electrónico desde alguna aplicación, ejecute:

```
setsebool -P httpd_can_sendmail 1
```

Para permitir que Apache pueda leer contenidos localizados en los directorios de inicio de los usuarios locales, ejecute:

```
setsebool -P httpd_read_user_content 1
```

Nota.

Estas últimas dos políticas son indispensables para el funcionamiento de cualquier cliente de correo electrónico basados sobre HTTP (*Webmails*).

Para permitir a Apache poder ejecutar guiones CGI, ejecute:

```
setsebool -P httpd_enable_cgi 1
```

Para permitir las inclusiones del lado del servidor (**SSI**, **S**erver **S**ide **I**ncludes), ejecute:

```
setsebool -P httpd_ssi_exec 1
```

Para permitir que Apache se pueda conectar a un base de datos localizada en otro servidor, ejecute:

```
setsebool -P httpd_can_network_connect_db 1
```

Para permitir a Apache realizar conexiones de red hacia otro servidor, ejecute:

```
setsebool -P httpd_can_network_connect 1
```

Para permitir que los usuarios locales puedan utilizar un directorio público (**public_html**), ejecute:

```
setsebool -P httpd_enable_homedirs 1
```

Nota.

Esta última política es indispensable para el funcionamiento de anfitriones virtuales asignados a usuarios locales, pues permite utilizar los directorios **~/public_html**.

Para permitir administrar a través de FTP o FTPS cualquier directorio gestionado por Apache o bien permitir a Apache funcionar como un servidor FTP escuchando peticiones a través del puerto de FTP, ejecute el siguiente mandato:

```
setsebool -P httpd_enable_ftp_server 1
```

Para **desactivar** la ejecución de PHP y otros lenguajes de programación para HTTP a través de Apache, ejecute el siguiente mandato:

```
setsebool -P httpd_builtin_scripting 0
```

Para consultar todas políticas disponibles que existen para Apache, ejecute:

```
getsebool -a |grep httpd
```

Para consultar todas políticas disponibles que existen para Apache, junto con una breve descripción, ejecute:

```
semanage boolean -l |grep httpd
```

Para definir que un directorio fuera de **/var/www**, como por ejemplo **/sitios/dominio.tld/html**, pueda ser utilizado por Apache, se le debe asignar el contexto **httpd_sys_content_t**. Éste puede asignarse a través del mandato **chcon**, como se muestra en el siguiente ejemplo:

```
chcon -t httpd_sys_content_t /sitios/dominio.tld/html
```

Cualquier contenido que sea **copiado** o **transferido** dentro de **/var/www** automáticamente adquiere el contexto **httpd_sys_content_t**.

Para definir que se permite ejecutar un guión CGI en particular, como por ejemplo **/sitios/dominio/cgi-bin/formulario.pl**, se utiliza el siguiente mandato:

```
chcon -t httpd_sys_script_exec_t /sitios/dominio/cgi-bin/formulario.pl
```

Cualquier contenido que sea **copiado** o **transferido** dentro de cualquier sub-directorio de **/var/www** que se denomine **cgi-bin**, automáticamente adquiere el contexto **httpd_sys_script_exec_t**.

Para definir que, por ejemplo, **/var/www/dominio/public_html/escribir.php** pueda realizar procedimientos de sólo lectura de datos fuera del directorio **/var/www**, ejecute el siguiente mandato:

```
chcon -t httpd_sys_script_ro_t /var/www/dominio/public_html/leer.php
```

Para definir que, por ejemplo, **/var/www/dominio/public_html/escribir.php** pueda realizar procedimientos de lectura y escritura de datos fuera del directorio **/var/www**, ejecute el siguiente mandato:

```
chcon -t httpd_sys_script_rw_t /var/www/dominio/public_html/leer.php
```

74.5. Modificaciones necesarias en el muro cortafuegos.

Es necesario abrir el puerto 80 por TCP (**HTTP**).

74.5.1. Servicio iptables.

Puede utilizar **iptables**, ejecutando lo siguiente:

```
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT

service iptables save
```

O bien edite el archivo **/etc/sysconfig/iptables**:

```
vim /etc/sysconfig/iptables
```

Y añada el siguiente contenido:

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
```

Y reinicie el servicio **iptables**:

```
service iptables restart
```

74.5.2. Shorewall.

Edite el archivo **/etc/shorewall/rules**:

```
vim /etc/shorewall/rules
```

Las reglas corresponderían a algo similar a lo siguiente, permitiendo el acceso hacia el servicio HTTP desde cualquier zona del muro cortafuegos:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  all     fw      tcp     80
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Para aplicar los cambios en Shorewall, ejecute lo siguiente:

```
service shorewall restart
```

74.6. Procedimientos.

74.6.1. Archivos de configuración.

Cualquier ajuste que se requiera realizar, ya sea para configurar anfitriones virtuales, u otra funcionalidad adicional, se puede realizar sin tocar el archivo principal de configuración (**/etc/httpd/conf/httpd.conf**), utilizando cualquier archivo con extensión ***.conf** dentro del directorio **/etc/httpd/conf.d/**.

74.6.2. UTF-8 y codificación de documentos.

UTF-8
: UTF-8 es un método de codificación de ASCII para Unicode (ISO-10646), el Conjunto de Caracteres Universal o UCS. éste codifica la mayoría de los sistemas de escritura del mundo en un único conjunto de caracteres, permitiendo la mezcla de lenguajes y guiones en un mismo documento sin la necesidad de ajustes para realizar los cambios de conjuntos de caracteres.

Debido a su conveniencia actualmente se está adoptando UTF-8 como codificación para todo, sin embargo aún hay mucho material codificado en, por ejemplo, ISO-8859-1.

Lo correcto es cambiar a en UTF-8 la codificación de los documentos que están en ISO8859-1, u otras tablas de caracteres, utilizando métodos similares el siguiente:

```
cd /var/www/html/
for f in *.html
do
vi -c ":wq! ++enc=utf8" $f
done
```

Lo anterior sólo tendría sentido si dentro del directorio **/var/www/html** hubiera documentos HTML codificados en ISO8859-1.

Si desea continuar **viviendo en el pasado** y no aceptar el nuevo estándar, también puede desactivar la función en Apache que establece UTF-8 como codificación predefinida. Edite el archivo **/etc/httpd/conf/httpd.conf**:

```
vim /etc/httpd/conf/httpd.conf
```

Localice lo siguiente:

```
AddDefaultCharset UTF-8
```

Cambie **UTF-8** por **Off**:

```
AddDefaultCharset Off
```

74.6.3. Directorios virtuales.

Si, por ejemplo, se quisiera añadir el alias para un directorio localizado en **/var/contenidos/ejemplo/** y el cual queremos visualizar como el directorio **/ejemplo/** en Apache, lo primero será crear el directorio:

```
mkdir -p /var/contenidos/ejemplo
```

Cambie los contextos de SELinux de este directorio, con la finalidad de que tenga rol de objeto (**object_r**), creado por usuario de sistema (**system_u**) y tipo **httpd_sys_content_t**:

```
chcon -u system_u /var/contenidos/ejemplo
chcon -r object_r /var/contenidos/ejemplo
chcon -t httpd_sys_content_t /var/contenidos/ejemplo
```

Genere el archivo **/etc/httpd/conf.d/ejemplos.conf**:

```
vim /etc/httpd/conf.d/ejemplos.conf
```

Añada el siguiente contenido:

```
Alias  /ejemplo  /var/contenidos/ejemplo
```

Guarde y cierre el archivo.

Recargue el servicio httpd.

```
service httpd reload
```

Asumiendo que realizará la prueba desde el mismo anfitrión local, visualice este nuevo directorio virtual, con cualquier navegador, a través de *http://127.0.0.1/ejemplo/*. Se mostrará que el directorio existe, pero el acceso a éste está denegado.

Si desea realizar las comprobaciones desde el mismo anfitrión, puede utilizar el navegador Lynx.

```
lynx http://127.0.0.1/ejemplo/
```

Lo anterior deberá mostrar un error 403 (acceso denegado), pues el directorio carece de un archivo índice. Para poder acceder deberá haber un documento índice en el interior (index.html, index.php, etc) o bien que dicho directorio sea configurado para mostrar el contenido.

Edite de nuevo el archivo **/etc/httpd/conf.d/ejemplos.conf**:

```
vim /etc/httpd/conf.d/ejemplos.conf
```

Modifique el contenido para que quede del siguiente modo:

```
Alias /ejemplo /var/contenidos/ejemplo
        <Directory "/var/contenidos/ejemplo">
                Options Indexes
        </Directory>
```

La opción **Indexes** indica que se deberá mostrar el índice de contenido del directorio.

Recargue el servicio **httpd** para aplicar la configuración:

```
service httpd reload
```

Asumiendo que realizará la prueba desde el mismo anfitrión local, acceda hacia *http://127.0.0.1/ejemplo/* con cualquier navegador y visualice el resultado.

Si se requiere que este directorio tenga aún mayor funcionalidad, se pueden añadir más opciones, como por ejemplo **AllowOverride, Includes y FollowSymLinks, como se muestra en el siguiente ejemplo:**

```
Alias /ejemplo /var/contenidos/ejemplo
        <Directory "/var/contenidos/ejemplo">
                Options Indexes Includes FollowSymLinks
                AllowOverride all
        </Directory>
```

En el ejemplo anterior:

- La opción **FollowSymLinks** habilita el uso de enlaces simbólicos dentro del directorio. Sólo utilice ésta si necesita acceder a contenidos fuera del directorio a utilizar.
- La opción **Includes** especifica que se permite la utilización de los **SSI** (***S****erver* ***S****ide* ***I****ncludes*). Sólo utilice ésta si así lo requiere la aplicación o programa utilizado dentro este directorio.
- La opción **AllowOverride**, con el valor **all** posibilita utilizar archivos **.htaccess**, los cuales a su vez permiten aplicar opciones de directorio al vuelo, sin necesidad de modificar otros archivos de configuración.

Para que surtan efecto los cambios hechos a la configuración, recargue el servicio **httpd**:

```
service httpd reload
```

Asumiendo que realizará la prueba desde el mismo anfitrión local, acceda hacia *http://127.0.0.1/ejemplo/* con cualquier navegador y visualice el resultado.

Si desea realizar las comprobaciones desde el mismo anfitrión, puede utilizar el navegador Lynx.

```
lynx http://127.0.0.1/ejemplo/
```

74.6.4. Limitar el acceso a directorios por dirección IP.

Si se requiere limitar el acceso de un directorio en particular, para que éste esté disponible sólo hacia ciertas direcciones IP o bloques de red, defina algo como lo mostrado en el siguiente ejemplo:

```
Alias /ejemplo /var/contenidos/ejemplo
        <Directory "/var/contenidos/ejemplo">
                Order deny,allow
                Deny from all
                Allow from 127.0.0.0/8 192.168.70.0/25
                Options Indexes
                AllowOverride all
        </Directory>
```

El ejemplo anterior establece que el orden de acceso, donde primero se aplicarán las reglas de denegación y luego las que permitirán el acceso y que se denegará el acceso a todo el mundo, permitiendo el acceso sólo desde **127.0.0.0/8** y **192.168.70.0/25**.

Para que surtan efecto los cambios hechos a la configuración, recargue el servicio **httpd**:

```
service httpd reload
```

sumiendo que realizará la prueba desde el mismo anfitrión local, acceda hacia *http://127.0.0.1/ejemplo/* con cualquier navegador y visualice el resultado.

Si desea realizar las comprobaciones desde el mismo anfitrión, puede utilizar el navegador Lynx.

```
lynx http://127.0.0.1/ejemplo/
```

74.6.5. Limitar el acceso por usuario y contraseña.

La autenticación para directorios, contra un archivo que incluya nombres de usuario y claves de acceso, que también puede combinarse con el acceso por dirección IP, se realiza a través de la siguiente sintaxis:

```
AuthName "Acceso sólo para usuarios autorizados"
AuthType Basic
Require valid-user
AuthUserFile /cualquier/ruta/hacia/archivo/de/claves
```

Lo anterior puede ser incluido en la configuración existente para cualquier directorio o bien en archivo **.htaccess**.

Genere el directorio **/var/www/privado/** ejecutando lo siguiente:

```
mkdir -p /var/www/privado
```

Genere un archivo denominado arbitrariamente **/etc/httpd/conf.d/ejemplo-autenticar.conf**:

```
vim /etc/httpd/conf.d/ejemplo-autenticar.conf
```

Añada con el siguiente contenido:

```
Alias /privado /var/www/privado
<Directory "/var/www/privado">
        Options Indexes
        AllowOverride All
        Order allow,deny
        Allow from all
</Directory>
```

Para que surtan efecto los cambios hechos a la configuración, recargue el servicio **httpd**:

```
service httpd reload
```

Genere el archivo **/var/www/privado/.htaccess**.

```
vim /var/www/privado/.htaccess
```

Agregue el siguiente contenido:

```
AuthName "Sólo usuarios autorizados"
AuthType Basic
Require valid-user
AuthUserFile /var/www/claves
```

Genere el archivo de claves de acceso como **/var/www/claves**, ejecutando el siguiente procedimiento:

```
touch /var/www/claves
```

Cambie los permisos de sólo lectura y escritura para usuario y cambie la propiedad al usuario y grupo **apache**:

```
chmod 600 /var/www/claves
chown apache:apache /var/www/claves
```

Agregue algunos **usuarios virtuales** al archivo de claves, **/var/www/claves**, ejecutando el mandato **htpasswd**, usando como argumentos la ruta del archivo de claves de acceso y nombre del usuario a añadir o modificar:

```
htpasswd /var/www/claves fulano
htpasswd /var/www/claves mengano
htpasswd /var/www/claves perengano
htpasswd /var/www/claves zutano
```

Asumiendo que realizará la prueba desde el mismo anfitrión local, acceda con cualquier navegador hacia *http://127.0.0.1/privado/* y compruebe que funciona el acceso con autenticación, utilizando cualquiera de los dos usuarios virtuales que generó con el mandato **htpasswd**, es decir fulano o mengano.

Si desea realizar las comprobaciones desde el mismo anfitrión, puede utilizar el navegador Lynx.

```
lynx http://127.0.0.1/privado/
```

74.6.6. Asignación de directivas para PHP.

Suelen darse los casos donde una aplicación, escrita en **PHP**, requiere algunas directivas de **PHP** en particular. En muchos casos se llegan a necesitar variables que pueden comprometer la seguridad de otras aplicaciones hospedadas en el servidor. Para tal fin es que se puede evitar modificar el archivo **/etc/php.ini** utilizando el parámetro **php_flag** en un archivo **.htaccess**. La siguiente sintaxis es la siguiente:

```
php_flag directiva_php valor
```

74.6.6.1. Ejemplo

Se procederá a asignar las directivas **register_globals**, **magic_quotes_runtime**, **magic_quotes_gpc** y **upload_max_filesize** al directorio en la ruta **/var/www/aplicacion**, mismo que será visualizado desde Apache como *http://127.0.0.1/aplicacion/*. El valor para **register_globals** será **On** (requerido sólo por aplicaciones PHP muy antiguas o muy mal escritas), el valor para **magic_quotes_runtime** será **On**, el valor para **magic_quotes_gpc** será **On** y el valor para **upload_max_filesize** será **8M**.

Genere el directorio **/var/www/aplicacion** ejecutando lo siguiente:

```
mkdir /var/www/aplicacion
```

Genere el archivo **/etc/httpd/conf.d/ejemplo-directivas-php.conf** ejecutando lo siguiente:

```
vim /etc/httpd/conf.d/ejemplo-directivas-php.conf
```

Añada el siguiente contenido:

```
Alias /aplicacion /var/www/aplicacion
<Directory "/var/www/aplicacion">
        AllowOverride All
</Directory>
```

Genere el archivo **/var/www/aplicacion/.htaccess** realizando lo siguiente:

```
touch /var/www/aplicacion/.htaccess
```

Edite el archivo **/var/www/aplicacion/.htaccess** y agregue el siguiente contenido:

```
php_flag register_globals On
php_flag magic_quotes_gpc On
php_flag magic_quotes_runtime On
php_value upload_max_filesize 8M
```

Genere el archivo **/var/www/aplicacion/info.php**, una función que muestra toda la información acerca de **PHP** en el servidor, a fin de corroborar los valores de las directivas de **PHP** en relación al directorio, con el siguiente contenido:

```
<?php
     phpinfo();
?>
```

Para que surtan efecto los cambios hechos a la configuración, recargue el servicio **httpd**:

```
service httpd reload
```

Acceda con cualquier navegador de red hacia *http://127.0.0.1/aplicacion/info.php*.

Si desea realizar las comprobaciones desde el mismo anfitrión, puede utilizar el navegador Lynx.

```
lynx http://127.0.0.1/aplicacion/info.php
```

Corrobore que los valores para las variables de **PHP** para el directorio involucrado realmente han sido asignadas. En la sub-sección **PHP Core** de la sección **Configuration**, hay tres columnas. La primera, **Directive**, corresponde a la directivas **PHP**. La segunda, **Local Value**, corresponde a los valores de las directivas de **PHP** para el directorio actual. La tercera, **Master Value**, corresponde a los valores de las directivas predeterminadas que están definidas en el archivo **/etc/php.ini**.

Directive	Local Value	Master Value
magic_quotes_gpc	On	Off
magic_quotes_runtime	On	Off
register_globals	On	Off
upload_max_filesize	8M	2M

74.6.7. Re-dirección de directorios.

Cuando sea necesario, es posible configurar un directorio en particular para Apache redirija éste de modo transparente hacia cualquier otra dirección.

Genere el archivo denominado arbitrariamente como **/etc/httpd/conf.d/ejemplo-redireccion.conf**, reemplazando **http://mail.docminio.tld/** por cualquier dirección válida.

```
vim /etc/httpd/conf.d/ejemplo-redireccion.conf
```

Añada el siguiente contenido:

```
Redirect 301 /webmail http://mail.dominio.tld/
```

Guarde el archivo y regrese al intérprete de mandatos.

Para que surtan efecto los cambios hechos a la configuración, recargue el servicio **httpd**:

```
service httpd reload
```

En el ejemplo anterior, se indica que si se trata de acceder hacia el sub-directorio **/webmail** en el servidor, Apache deberá redirigir hacia *http://mail.dominio.tld/*. El número 301 corresponde al mensaje del protocolo HTTP para indicar que la re-dirección es permanente. Si por ejemplo hubiese un objeto en /webmail, como por ejemplo **/webmail/estadisticas/estadisticas.php**, Apache realizaría el re-direccionamiento transparente hacia *http://mail.dominio.tld/estadisticas/estadisticas.php*.

74.6.8. Tipos de MIME.

Para añadir cualquier tipo de extensión y tipo MIME, como por ejemplo Ogg, definiendo además una descripción e icono, genere un archivo que denominado **/etc/httpd/conf.d/mimes.conf**:

```
vim /etc/httpd/conf.d/mimes.conf
```

Añada el siguiente contenido:

```
AddType application/ogg .ogg
AddDescription "Ogg Vorbis Audio" .ogg
AddIcon /icons/sound2.png .ogg
```

Para que surtan efecto los cambios hechos a la configuración, recargue el servicio **httpd**:

```
service httpd reload
```

Copie o transfiera cualquier archivo de audio Ogg Vorbis a cualquier directorio compartido a través de Apache que permita ver el índice de éste y visualice el resultado.

74.6.9. Impedir enlace remoto de imágenes.

Suele ocurrir que los administradores de algunos sitios encuentran fácil utilizar imágenes y otros tipos de contenido, vinculando desde sus documentos hacia los objetos en el servidor. Ésto representa un consumo ancho de banda adicional para el servidor, que sólo genera tráfico inútil y por lo tanto es considerado una práctica poco ética. En el siguiente ejemplo se desea proteger un directorio para que sólo se permita utilizar su contenido si es referido desde el mismo servidor.

Genere el directivo **/var/www/imagenes** ejecutando lo siguiente:

```
mkdir /var/www/imagenes
```

Copie o transfiera archivos de imágenes dentro de este directorio.

```
cp /usr/share/pixmaps/*.png /var/www/imagenes
```

Genere el archivo **/etc/httpd/conf.d/imagenes.conf** ejecutando lo siguiente:

```
vim /etc/httpd/conf.d/imagenes.conf
```

Añada el siguiente contenido:

```
# Se permite acceder directamente a la imagen o bien si se omite
# en el navegador la información del referente.
SetEnvIfNoCase Referer "^$" local_referal=1
# Se permite al propio servidor
SetEnvIfNoCase Referer "^http://127.0.0.1" local_referal=1
SetEnvIfNoCase Referer "^http://localhost" local_referal=1
SetEnvIfNoCase Referer "^http://localhost.localdomain" local_referal=1
SetEnvIfNoCase Referer "^http://192.168.70.50" local_referal=1
SetEnvIfNoCase Referer "^http://m50.alcancelibre.org.mx" local_referal=1
SetEnvIfNoCase Referer "^http://(www.)?midominio.org" local_referal=1
# Se permite utilizar las imágenes a otro servidor
SetEnvIfNoCase Referer "^http://(www.)?sitio-amigo.org" local_referal=1

Alias /imagenes /var/www/imagenes
<Directory  "/var/www/imagenes">
        Order Deny,Allow
        Deny from all
        Allow from env=local_referal
</Directory>
```

Para que surtan efecto los cambios hechos a la configuración, recargue el servicio **httpd**:

```
service httpd reload
```

Pruebe la configuración creando un documento HTML en el anfitrión local y en un anfitrión remoto, el cual enlace hacia imágenes hospedadas en el directorio **/var/www/imagenes** del servidor recién configurado, y compare resultados.

En lugar de lo anterior, puede utilizarse también un archivo **.htaccess**. Edite el archivo **/etc/httpd/conf.d/imagenes.conf** ejecutando lo siguiente:

```
vim /etc/httpd/conf.d/imagenes.conf
```

Reemplace el contenido existente por lo siguiente:

```
Alias /imagenes /var/www/imagenes
<Directory  "/var/www/imagenes">
        AllowOverride all
</Directory>
```

Para que surtan efecto los cambios hechos a la configuración, recargue el servicio **httpd**:

```
service httpd reload
```

Genere el archivo **/var/www/imagenes/.htaccess**:

```
vim /var/www/imagenes/.htaccess
```

Añada el siguiente contenido:

```
# Se permite acceder directamente a la imagen o bien si se omite
# en el navegador la información del referente.
SetEnvIfNoCase Referer "^$" local_referal=1
# Se permite al propio servidor
SetEnvIfNoCase Referer "^http://127.0.0.1" local_referal=1
SetEnvIfNoCase Referer "^http://localhost" local_referal=1
SetEnvIfNoCase Referer "^http://localhost.localdomain" local_referal=1
SetEnvIfNoCase Referer "^http://192.168.70.50" local_referal=1
SetEnvIfNoCase Referer "^http://m50.alcancelibre.org.mx" local_referal=1
SetEnvIfNoCase Referer "^http://(www.)?midominio.org" local_referal=1
# Se permite utilizar las imágenes a otro servidor
SetEnvIfNoCase Referer "^http://(www.)?sitio-amigo.com" local_referal=1

Order Deny,Allow
Deny from all
Allow from env=local_referal
```

Pruebe la configuración creando un documento HTML en el anfitrión local y en un anfitrión remoto, el cual enlace hacia imágenes hospedadas en el directorio **/var/www/imagenes** del servidor recién configurado, y compare resultados.

75. Configuración de Apache con soporte SSL/TLS.

Autor: *Joel Barrios Dueña*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

75.1. Introducción.

75.1.1. Acerca de HTTPS.

HTTPS es la versión segura del protocolo **HTTP**, inventada en 1996 por Netscape Communications Corporation. Es es un protocolo dependiente de **HTTP**, consistiendo de una combinación de éste con un mecanismo de transporte **SSL** o **TLS**, garantizando así una protección razonable durante la comunicación cliente-servidor. Es ampliamente utilizado en la red mundial (**WWW** o **W**orld **W**ide **W**eb) para comunicaciones como transacciones bancarias y pago de bienes y servicios.

El servicio utiliza el puerto 443 por TCP para realizar las comunicaciones (la comunicación normal para HTTP utiliza el 80 por TCP). El esquema **URI** (**U**niform **R**esource **I**dentifier o Identificador Uniforme de Recursos) es, comparando sintaxis, idéntico al de **HTTP** (http:), utilizándose como **«https:»** seguido del subconjunto denominado **URL** (**U**niform **R**esource **L**ocator o Localizador Uniforme de Recursos). Ejemplo: *https://www.dominio.tld/*

URL: http://es.wikipedia.org/wiki/HTTPS y http://wp.netscape.com/eng/ssl3/draft302.txt

75.1.2. Acerca de RSA.

RSA, acrónimo de los apellidos de sus autores, Ron **R**ivest, Adi **S**hamir y Len **A**dleman, es un algoritmo para el ciframiento de claves públicas que fue publicado en 1977, patentado en EE.UU. en 1983 por el el Instituto Tecnológico de Michigan (**MIT**). **RSA** es utilizado ampliamente en todo el mundo para los protocolos destinados para el comercio electrónico.

URL: http://es.wikipedia.org/wiki/RSA

75.1.3. Acerca de Triple DES.

Triple DES o **TDES**, es un algoritmo que realiza un triple cifrado DES, desarrollado por IBM en 1978. Su origen tuvo como finalidad el agrandar la longitud de una clave sin necesidad de cambiar el algoritmo de ciframiento, lo cual lo hace más seguro que el algoritmo **DES**, obligando a un atacante el tener que triplicar el número de operaciones para poder hacer daño. A pesar de que actualmente está siendo reemplazado por el algoritmo **AES** (**A**dvanced **E**ncryption **S**tandard, también conocido como **Rijndael**), sigue siendo estándar para las tarjetas de crédito y operaciones de comercio electrónico.

URL: http://es.wikipedia.org/wiki/Triple_DES

75.1.4. Acerca de X.509.

X.509 es un estándar **ITU-T** (estandarización de **T**elecomunicaciones de la **I**nternational **T**elecommunication **U**nion) para infraestructura de claves públicas (**PKI** o **P**ublic **K**ey **I**nfrastructure). Entre otras cosas, establece los estándares para certificados de claves públicas y un algoritmo para validación de ruta de certificación. Este último se encarga de verificar que la ruta de un certificado sea válida bajo una infraestructura de clave pública determinada. Es decir, desde el certificado inicial, pasando por certificados intermedios, hasta el certificado de confianza emitido por una Autoridad Certificadora (**CA** o **C**ertification **A**uthority).

URL: http://es.wikipedia.org/wiki/X.509

75.1.5. Acerca de OpenSSL.

OpenSSL es una implementación libre, de código abierto, de los protocolos **SSL** (**S**ecure **S**ockets **L**ayer o Nivel de Zócalo Seguro) y **TLS** (**T**ransport **L**ayer **S**ecurity o Seguridad para Nivel de Transporte). Está basado sobre el extinto proyecto **SSLeay**, iniciado por Eric Young y Tim Hudson, hasta que éstos comenzaron a trabajar para la división de seguridad de EMC Corporation.

URL: http://www.openssl.org/

75.1.6. Acerca de mod_ssl.

Mod_ssl es un módulo para el servidor HTTP Apache, el cual provee soporte para SSL versiones 2 y 3 y TLS versión 1. Es una contribución de Ralf S. Engeschall, derivado del trabajo de Ben Laurie.

URL: http://www.apache-ssl.org/ y http://httpd.apache.org/docs/2.2/mod/mod_ssl.html

75.2. Requisitos.

Es necesario disponer de una dirección IP pública para cada sitio de red virtual que se quiera configurar con soporte **SSL**/**TLS**. Debido a la naturaleza de los protocolos **SSL** y **TLS**, es imposible utilizar múltiples anfitriones virtuales con soporte **SSL**/**TLS** utilizando una misma dirección IP. Cada certificado utilizado requerirá una dirección IP independiente en el anfitrión virtual.

El paquete **mod_ssl** instala el archivo **/etc/httpd/conf.d/ssl.conf**, mismo que es innecesario modificar si se utilizan archivos de inclusión, con extensión *.conf, dentro del directorio **/etc/httpd/conf.d/**. Ésto se recomienda a fin de preservar la configuración predeterminada y poder disponer de ésta, brindando un punto de retorno en el caso de que alguna configuración diese problemas, limitándose solo a modificar los parámetros del archivo ssl.conf para configurar las rutas del certificado y firma digital.

75.3. Equipamiento lógico necesario.

75.3.1. Instalación a través de yum.

Si se utiliza de **CentOS** o bien **Red Hat Enterprise Linux**, ejecute lo siguiente:

```
yum -y install mod_ssl
```

75.4. Procedimientos.

75.4.1. Generando firma digital y certificado.

Acceda al sistema como el usuario **root**.

Acceda al directorio **/etc/pki/tls/**.

```
cd /etc/pki/tls
```

En caso de que existieran previamente, debe eliminar los archivos **certs/dominio.tld.crt**, **certs/dominio.tld.crs**, **private/dominio.tld.key** y **private/dominio.tld.pem**.

```
rm -f certs/dominio.tld.crt private/dominio.tld.key
rm -f certs/dominio.tld.csr private/dominio.tld.pem
```

Se debe crear una clave con algoritmo **RSA** de 2048 octetos y estructura **x509**, la cual se cifra utilizado **Triple DES** (**D**ata **E**ncryption **S**tandard), almacenado en formato **PEM** de modo que sea interpretable como texto ASCII. se solicitará una clave de acceso para asignar a la firma digital, por lo que **se recomienda utilizar una muy buena clave de acceso**, la cual, mientras más complicada y difícil sea, mejor.

```
openssl genrsa -des3 -out private/dominio.tld.key 2048
```

Si se utiliza este archivo (dominio.tld.key) para la configuración del anfitrión virtual, se requerirá de interacción del administrador cada vez que se tenga que iniciar o reiniciar, el servicio httpd, ingresando la clave de acceso de la firma digital. Este es el procedimiento más seguro, sin embargo, debido a que resultaría poco práctico tener que ingresar una clave de acceso cada vez que se inicie el servicio httpd, resulta más conveniente generar una firma digital **RSA**, la cual permita iniciar normalmente y sin interacción alguna, al servicio httpd.

```
openssl rsa -in private/dominio.tld.key -out private/dominio.tld.pem
```

El archivo **dominio.tld.pem** será el que se especifique más adelante como valor del parámetro **SSLCertificateKeyFile** en la configuración de Apache.

A continuación, genere el archivo **CSR** (**C**ertificate **S**igning **R**equest), el cual es el archivo de solicitud que se hace llegar a una **RA** (**R**egistration **A**uthority o Autoridad de Registro), como **Verisign**, quienes, tras el correspondiente pago, envían de vuelta un certificado (para ser utilizado como el archivo **dominio.tld.crt**) firmado por dicha autoridad certificadora.

```
openssl req -new -key private/dominio.tld.key -out certs/dominio.tld.csr
```

Lo anterior solicitará se ingresen varios datos:

- Código de dos letras para el país.
- Estado o provincia.
- Ciudad.
- Nombre de la empresa o razón social.
- Unidad o sección.

- Nombre del anfitrión. Debe ser el nombre con el que se accederá hacia el servidor y dicho nombre deberá estar resuelto en un DNS. SI lo desea, puede utilizar también ***.dominio.tld**.
- Dirección de correo electrónico válida del administrador del sistema.
- De manera opcional se puede añadir otra clave de acceso y nuevamente el nombre de la empresa. Poco recomendado, a menos que quiera ingresar ésta cada vez que se inicie o reinicie el servicio **httpd**.

La salida devuelta sería similar a la siguiente:

```
You are about to be asked to enter information that will be
incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or
a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:MX
State or Province Name (full name) [Berkshire]:Distrito Federal
Locality Name (eg, city) [Newbury]:Mexico
Organization Name (eg, company) [My Company Ltd]:Empresa, S.A. de C.V.
Organizational Unit Name (eg, section) []:Direccion Comercial
Common Name (eg, your name or your server's hostname) []:*.dominio.tld
Email Address []:webmaster@dominio.tld

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Si requiere un **certificado auto-firmado**, en lugar de un certificado firmado por un **RA**, puede generarse éste utilizando el archivo de petición **CSR** (dominio.tld.csr). En el ejemplo a continuación, se crea un certificado con estructura X.509 en el que se establece una validez por 730 días (dos años).

```
openssl x509 -req -days 730 -in certs/dominio.tld.csr -signkey private/dominio.tld.key -out
certs/dominio.tld.crt
```

Con la finalidad de que sólo el usuario **root** pueda acceder a los archivos creados, se deben cambiar los permisos de éstos a sólo lectura para **root**.

```
chmod 400 private/dominio.tld.key private/dominio.tld.pem
chmod 400 certs/dominio.tld.csr certs/dominio.tld.crt
```

75.4.2. Configuración simple de Apache para un solo dominio.

Edite el archivo **/etc/httpd/conf.d/ssl.conf**:

```
vim /etc/httpd/conf.d/ssl.conf
```

Localice lo siguiente:

```
#   Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate.  If
# the certificate is encrypted, then you will be prompted for a
# pass phrase.  Note that a kill -HUP will prompt again.  A new
# certificate can be generated using the genkey(1) command.
SSLCertificateFile /etc/pki/tls/certs/localhost.crt

#   Server Private Key:
#   If the key is not combined with the certificate, use this
#   directive to point at the key file.  Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
```

Cambie **localhost.crt** y **localhost.key**, por **dominio.tld.crt** y **dominio.tld.pem**:

```
#   Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate.  If
# the certificate is encrypted, then you will be prompted for a
# pass phrase.  Note that a kill -HUP will prompt again.  A new
# certificate can be generated using the genkey(1) command.
SSLCertificateFile /etc/pki/tls/certs/dominio.tld.crt

#   Server Private Key:
#   If the key is not combined with the certificate, use this
#   directive to point at the key file.  Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile /etc/pki/tls/private/dominio.tld.pem
```

A fin de que surtan efecto los cambios, es necesario reiniciar el servicio **httpd**.

```
service httpd restart
```

Lo anterior deberá de proceder sin solicitar la clave de acceso de la firma digital (la que asignó cuando se creo **dominio.tld.key**). En caso contrario, significa que estableció **dominio.tld.key** como valor del parámetro **SSLCertificateKeyFile** en la configuración de Apache.

75.4.3. Configuración de Apache para múltiples dominios.

Omita el procedimiento anterior.

Es importante resaltar que cada dominio deberá contar con su propia dirección IP, pues el protocolo HTTPS impedirá utilizar más de un certificado por dirección IP.

El primer paso consiste en crear la estructura de directorios para el anfitrión virtual.

```
mkdir -p /var/www/dominio.tld/{cgi-bin,html,logs,etc}
```

De todos directorios creados, sólo **/var/www/dominio.tld/html**, **/var/www/dominio.tld/etc** y **/var/www/dominio.tld/cgi-bin** pueden pertenecer a un usuario sin privilegios, quien administrará este anfitrión virtual.

Crear el archivo **/etc/httpd/conf.d/dominio.conf**:

```
vim /etc/httpd/conf.d/dominio.conf
```

Adaptar la siguiente plantilla como contenido de este archivo, donde **a.b.c.d** corresponde a una dirección IP y **dominio.tld** corresponde al nombre de dominio a configurar para el anfitrión virtual:

```
### dominio.tld ###
NameVirtualHost a.b.c.d:80
        <VirtualHost a.b.c.d:80>
                ServerAdmin webmaster@dominio.tld
                DocumentRoot /var/www/dominio.tld/html
                ServerName www.dominio.tld
                ServerAlias dominio.tld
                Redirect 301 / https://www.dominio.tld/
                CustomLog logs/dominio.tld-access_log combined
                Errorlog logs/dominio.tld-error_log
        </VirtualHost>

NameVirtualHost a.b.c.d:443
        <VirtualHost a.b.c.d:443>
                ServerAdmin webmaster@dominio.tld
                DocumentRoot /var/www/dominio.tld/html
                ServerName www.dominio.tld
                ScriptAlias /cgi-bin/ /var/www/dominio.tld/cgi-bin/
                <Directory "/var/www/dominio.tld/cgi-bin">
                        SSLOptions +StdEnvVars
                </Directory>
                SSLEngine on
                SSLProtocol all -SSLv2
                SSLCipherSuite ALL:!ADH:!EXPORT:!SSLv2:RC4+RSA:+HIGH:+MEDIUM:+LOW
                SSLCertificateFile /etc/pki/tls/certs/dominio.tld.crt
                SSLCertificateKeyFile /etc/pki/tls/private/dominio.tld.pem
                SetEnvIf User-Agent ".*MSIE.*" \
                        nokeepalive ssl-unclean-shutdown \
                        downgrade-1.0 force-response-1.0
                CustomLog logs/dominio.tld-ssl_request_log \
                        "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
                Errorlog logs/dominio.tld-ssl_error_log
                TransferLog logs/dominio.tld-ssl_access_log
                LogLevel warn
        </VirtualHost>
```

A fin de que surtan efecto los cambios, es necesario reiniciar el servicio **httpd**.

```
service httpd restart
```

Lo anterior deberá de proceder sin solicitar la clave de acceso de la firma digital (la que asignó cuando se creo **dominio.tld.key**). En caso contrario, significa que estableció **dominio.tld.key** como valor del parámetro **SSLCertificateKeyFile** en la configuración de Apache.

75.4.4. Comprobación.

Sólo basta dirigir cualquier navegador HTTP hacia **https://www.dominio.tld/** a fin de verificar que todo esté trabajando correctamente. Tras aceptar el certificado, en el caso de que éste no haya sido firmado por un **RA**, deberá poderse observar un signo en la barra de estado del navegador, el cual indica que se trata de una conexión segura.

75.4.5. Modificaciones necesarias en el muro cortafuegos.

Si se utiliza un cortafuegos, es necesario abrir, además del puerto 80 por TCP (**HTTP**), el puerto 443 por TCP (**HTTPS**).

Si utiliza **Shorewall**, edite el archivo **/etc/shorewall/rules**:

```
vim /etc/shorewall/rules
```

Las reglas corresponderían a algo similar a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  all     fw      tcp     80,443
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Al terminar de configurar las reglas para **Shorewall**, reinicie el muro cortafuegos, ejecutando el siguiente mandato:

```
service shorewall restart
```

76. Configuración de Squid: Opciones básicas.

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

76.1. Introducción.

76.1.1. ¿Qué es Servidor Intermediario (Proxy)?

El término en ingles **«Proxy»** tiene un significado muy general y al mismo tiempo ambiguo, aunque invariablemente se considera un sinónimo del concepto de **«Intermediario»**. Se suele traducir, en el sentido estricto, como **delegado** o **apoderado** (el que tiene poder sobre otro).

Un **Servidor Intermediario** se define como una computadora o dispositivo que ofrece un servicio de red que consiste en permitir a los clientes realizar conexiones de red indirectas hacia otros servicios de red. Durante el proceso ocurre lo siguiente:

1. Cliente se conecta hacia un **Servidor Proxy**.
2. Cliente solicita una conexión, archivo u otro recurso disponible en un servidor distinto.
3. Servidor Intermediario proporciona el recurso ya sea conectándose hacia el servidor especificado o sirviendo éste desde un caché.
4. En algunos casos el **Servidor Intermediario** puede alterar la solicitud del cliente o bien la respuesta del servidor para diversos propósitos.

Los **Servidores Proxy** generalmente se hacen trabajar simultáneamente como muro cortafuegos operando en el **Nivel de Red**, actuando como filtro de paquetes, como en el caso de **iptables** o bien operando en el **Nivel de Aplicación**, controlando diversos servicios, como es el caso de **TCP Wrapper**. Dependiendo del contexto, el muro cortafuegos también se conoce como **BPD** o **B**order **P**rotection **D**evice o simplemente **filtro de paquetes**.

Una aplicación común de los **Servidores Proxy** es funcionar como caché de contenido de Red (principalmente HTTP), proporcionando en la proximidad de los clientes un caché de páginas y archivos disponibles a través de la Red en servidores HTTP remotos, permitiendo a los clientes de la red local acceder hacia éstos de forma más rápida y confiable.

Cuando se recibe una petición para un recurso de Red especificado en un **URL** (**U**niform **R**esource **L**ocator) el **Servidor Intermediario** busca el resultado del **URL** dentro del caché. Si éste es encontrado, el **Servidor Intermediario** responde al cliente proporcionado inmediatamente el contenido solicitado. Si el contenido solicitado estuviera ausente en el caché, el **Servidor Intermediario** lo traerá desde servidor remoto, entregándolo al cliente que lo solicitó y guardando una copia en el caché. El contenido en el caché es eliminado luego a través de un algoritmo de expiración de acuerdo a la antigüedad, tamaño e historial de **respuestas a solicitudes** (hits) (ejemplos: **LRU**, **LFUDA** y **GDSF**).

Los **Servidores Proxy** para contenido de Red (Web Proxies) también pueden actuar como filtros del contenido servido, aplicando políticas de censura de acuerdo a criterios arbitrarios.

76.1.2. Acerca de Squid.

Squid es un **Servidor Intermediario** de alto desempeño que se ha venido desarrollando desde hace varios años y es hoy en día un muy popular y ampliamente utilizado entre los sistemas operativos como GNU/Linux y derivados de Unix®. Es muy confiable, robusto y versátil y se distribuye bajo los términos de la Licencia Pública General GNU (**GNU/GPL**). Siendo equipamiento lógico **libre**, está disponible el código fuente para quien así lo requiera.

Entre otras cosas, **Squid** puede funcionar como **Servidor Intermediario** y **caché de contenido de Red** para los protocolos **HTTP**, **FTP**, **GOPHER** y **WAIS**, Proxy de **SSL**, caché transparente, **WWCP**, aceleración **HTTP**, caché de consultas DNS y otras muchas más como filtración de contenido y control de acceso por IP y por usuario.

Squid consiste de un programa principal como servidor, un programa para búsqueda en servidores **DNS**, programas opcionales para reescribir solicitudes y realizar autenticación y algunas herramientas para administración y herramientas para clientes. Al iniciar **Squid** da origen a un número configurable (5, de modo predeterminado a través dla opción **dns_children**) de procesos de búsqueda en servidores **DNS**, cada uno de los cuales realiza una búsqueda única en servidores **DNS**, reduciendo la cantidad de tiempo de espera para las búsquedas en servidores **DNS**.

Nota.

Squid carece de soporte para ser utilizado como Servidor Proxy para protocolos como **SMTP**, **POP3**, **TELNET**, **SSH**, **IRC**, etc. Si se requiere intermediar para **cualquier protocolo distinto** a **HTTP**, **HTTPS**, **FTP**, **GOPHER** y **WAIS** se requerirá implementar obligatoriamente un enmascaramiento de IP o **NAT** (**N**etwork **A**ddress **T**ranslation) o bien hacer uso de un servidor **SOCKS** como **Dante** (http://www.inet.no/dante/).

URL: http://www.squid-cache.org/

76.2. Equipamiento lógico necesario.

Para poder llevar al cabo los procedimientos descritos en este y otros documentos relacionados, se requiere instalar al menos lo siguiente:

- Al menos squid-2.5.STABLE6
- **Todos** los parches de seguridad disponibles para la versión del sistema operativo que esté utilizando.
- Un muro cortafuegos configurado con **system-config-firewall**, **Firestarter** o **Shorewall**.

Squid sólo se instala de manera predeterminada cuando se instala el grupo de paquetes denominado «**Servidor Web**». El procedimiento de instalación es exactamente el mismo que con cualquier otro equipamiento lógico.

76.2.1. Instalación a través de yum.

Si se utiliza **CentOS** o **Red Hat™ Enterprise Linux**, ejecute:

```
yum -y install squid
```

76.3. SELinux y el servicio squid.

En **CentOS 6** y **Red Hat™ Enterprise Linux 6**, la política **squid_connect_any** viene habilitada de modo predeterminado. En **CentOS 5** y **Red Hat™ Enterprise Linux 5**, esta política viene deshabilitada de modo predeterminado. Esta política hace que SELinux permita a Squid aceptar conexiones de los clientes desde cualquier dirección IP. Si utiliza **CentOS 5** y **Red Hat™ Enterprise Linux 5**, ejecute:

```
setsebool -P squid_connect_any 1
```

Para SELinux permita a Squid operar en modo transparente en **CentOS 6** y **Red Hat™ Enterprise Linux 6**, ejecute:

```
setsebool -P squid_use_tproxy 1
```

Nota.

En **CentOS 5** y **Red Hat™ Enterprise Linux 5**, se pude utilizar una política adicional. Para que SELinux permita al servicio **squid** funcionar normalmente, haciendo que todo lo anteriormente descrito en esta sección pierda sentido, ejecute:

```
setsebool -P squid_disable_trans 1
```

76.4. Antes de continuar.

Evite dejar **espacios vacíos** en lugares indebidos. El siguiente ejemplo muestra la manera incorrecta de habilitar un opción.

Mal

```
# Opción incorrectamente habilitada.
  http_port 8080
```

El siguiente ejemplo muestra la manera correcta de habilitar un opción.

Bien

```
# Opción correctamente habilitada.
http_port 8080
```

76.5. Configuración básica.

Squid utiliza el archivo de configuración localizado en **/etc/squid/squid.conf** y podrá trabajar sobre este utilizando su editor de texto simple preferido. Existen un gran número de opciones, de los cuales recomendamos configurar los siguientes:

- Al menos una **Lista de Control de Acceso**
- Al menos una **Regla de Control de Acceso**
- http_port
- cache_dir
- error_directory, sólo si va a personalizar mensajes de error.

El resto de los opciones mencionados en este documento son, valga la redundancia, opcionales.

Edite el archivo **/etc/squid/squid.conf**:

```
vi /etc/squid/squid.conf
```

76.5.1. Controles de acceso.

Parapoder controlar el tráfico de los clientes hacia Internet, es necesario establecer **Listas de Control de Acceso** que definan una red o bien ciertos anfitriones en particular. A cada lista se le asignará una **Regla de Control de Acceso** que permitirá o denegará el acceso a **Squid**.

76.5.1.1. Listas de control de acceso.

De modo predeterminado en **CentOS 6** y **Red Hat™ Enterprise Linux 6**, Squid habilita el acceso a todas las redes locales, definidas en el RFC1918. Es decir, permite el acceso a 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, fc00::/7 y fe80::/10.

```
# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
acl localnet src 10.0.0.0/8     # RFC1918 possible internal network
acl localnet src 172.16.0.0/12  # RFC1918 possible internal network
acl localnet src 192.168.0.0/16 # RFC1918 possible internal network
acl localnet src fc00::/7   # RFC 4193 local private network range
acl localnet src fe80::/10  # RFC 4291 link-local (directly plugged) machines
```

Deshabilite todo lo anterior, colocando una almoadilla (# al inicio de cada línea.

```
# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
# acl localnet src 10.0.0.0/8     # RFC1918 possible internal network
# acl localnet src 172.16.0.0/12  # RFC1918 possible internal network
# acl localnet src 192.168.0.0/16 # RFC1918 possible internal network
# acl localnet src fc00::/7   # RFC 4193 local private network range
# acl localnet src fe80::/10  # RFC 4291 link-local (directly plugged) machines
```

Regularmente una lista de control de acceso se establece con la siguiente sintaxis:

```
acl [nombre de la lista] src [lo que compone a la lista]
```

Si se desea establecer una lista de control de acceso que abarque a toda la red local, basta definir la IP correspondiente a la red y la máscara de la sub-red. Por ejemplo, si se tiene una red donde los anfitriones tienen direcciones del segmento IP 172.16.100.0/28, se puede utilizar lo siguiente:

```
acl localnet src 172.16.100.0/28
```

También puede definirse una **Lista de Control de Acceso** especificando un archivo localizado en cualquier parte del disco duro y la cual contiene una lista de direcciones IP. Ejemplo:

```
acl permitidos src "/etc/squid/listas/permitidos"
```

El archivo **/etc/squid/listas/permitidos** tendría un contenido similar al siguiente:

```
172.16.100.1
172.16.100.2
172.16.100.3
172.16.100.15
172.16.100.16
172.16.100.20
172.16.100.40
```

Lo anterior estaría definiendo que la **Lista de Control de Acceso** denominada **permitidos** estaría compuesta por las direcciones IP incluidas en el archivo **/etc/squid/listas/permitidos**.

76.5.1.2. Reglas de Control de Acceso.

Estas definen si se permite o deniega acceso hacia **Squid**. Se aplican a las **Listas de Control de Acceso**. Deben colocarse en la sección de reglas de control de acceso definidas por el administrador, es decir, a partir de donde se localiza la siguiente leyenda:

```
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
```

La sintaxis básica de una regla de control de acceso es la siguiente:

```
http_access [deny o allow] [lista de control de acceso]
```

Para desactivar la configuración predeterminada y poder utilizar una diferente, localice La línea que incluye **http_access allow localnet**:

```
# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
http_access allow localnet
http_access allow localhost
```

Deshabilite esta línea colocando una almohadilla (# al inicio de ésta:

```
# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
# http_access allow localnet
http_access allow localhost
```

En el siguiente ejemplo se considera una regla que establece acceso permitido a **Squid** a la **Lista de Control de Acceso** denominada **permitidos**:

```
http_access allow permitidos
```

También pueden definirse reglas valiéndose de la expresión **!**, la cual significa **no**. Pueden definirse, por ejemplo, dos listas de control de acceso, una denominada **lista1** y otra denominada **lista2**, en la misma regla de control de acceso, en donde se asigna una expresión a una de estas. La siguiente establece que se permite el acceso a **Squid** a lo que comprenda **lista1** excepto aquello que comprenda **lista2**:

```
http_access allow lista1 !lista2
```

Este tipo de reglas son útiles cuando se tiene un gran grupo de IP dentro de un rango de red al que se debe **permitir** acceso y otro grupo dentro de la misma red al que se debe **denegar** el acceso.

76.5.2. Aplicando Listas y Reglas de control de acceso.

Una vez comprendido el funcionamiento de la Listas y las Regla de Control de Acceso, se procede a determinar cuales utilizar para la configuración.

76.5.2.1. Caso 1.

Considerando como ejemplo que se dispone de una red 172.16.100.0/28, si se desea definir toda la red local, se utilizaría la siguiente línea en la sección de **Listas de Control de Acceso**:

```
acl localnet src 172.16.100.0/28
```

Habiendo hecho lo anterior, la sección de listas de control de acceso debe quedar más o menos del siguiente modo:

Listas de Control de Acceso: definición de una red local completa

```
#
# Recommended minimum configuration:
acl all src 0.0.0.0/0
acl manager proto cache_object
acl localhost src 127.0.0.1/8
acl localnet src 172.16.100.0/28
```

A continuación se procede a aplicar la regla de control de acceso:

```
http_access allow localnet
```

Habiendo hecho lo anterior, la zona de reglas de control de acceso debería quedar de modo similar al siguiente:

Reglas de control de acceso: Acceso a una Lista de Control de Acceso.

```
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
http_access allow localhost
http_access allow localnet
http_access deny all
```

La regla **http_access allow localnet** permite el acceso a **Squid** a la **Lista de Control de Acceso** denominada **localnet**, la cual, en el siguiente ejemplo, está conformada por 172.16.100.0/28. Esto significa que cualquier anfitrión desde 172.16.100.1 hasta 172.16.100.14 podrá acceder a **Squid**.

76.5.2.2. Caso 2.

Si sólo se desea permitir el acceso a **Squid** a ciertas direcciones IP de la red local, deberemos crear un archivo que contenga dicha lista. Genere el archivo **/etc/squid/listas/localnet**, dentro del cual se incluirán sólo aquellas direcciones IP que desea confirmen la Lista de Control de acceso. Ejemplo:

```
172.16.100.1
172.16.100.2
172.16.100.3
172.16.100.4
172.16.100.5
172.16.100.6
172.16.100.7
```

Denominaremos a esta lista de control de acceso como **localnet**:

```
acl localnet src "/etc/squid/listas/localnet"
```

Habiendo hecho lo anterior, la sección de listas de control de acceso debe quedar más o menos del siguiente modo:

Listas de Control de Acceso: definición de una red local completa

```
#
# Recommended minimum configuration:
acl all src 0.0.0.0/0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl localnet src "/etc/squid/listas/localnet"
```

A continuación se procede a aplicar la regla de control de acceso:

```
http_access allow localnet
```

Habiendo hecho lo anterior, la zona de reglas de control de acceso debería quedar de modo similar al siguiente:

Reglas de control de acceso: Acceso a una Lista de Control de Acceso.

```
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
http_access allow localhost
http_access allow localnet
http_access deny all
```

La regla **http_access allow localnet** permite el acceso a **Squid** a la **Lista de Control de Acceso** denominada **localnet**, la cual está conformada por las direcciones IP especificadas en el archivo **/etc/squid/listas/localnet**. Esto significa que cualquier anfitrión excluido del archivo **/etc/squid/listas/localnet** se le denegará el acceso a **Squid**.

76.5.3. Opción cache_mgr.

Esta opción es de carácter informativo. De modo predeterminado, si algo ocurre con el caché, como por ejemplo que muera el procesos, se enviará un mensaje de aviso a la cuenta **webmaster** del servidor. Puede especificarse una distinta si acaso se considera conveniente.

```
cache_mgr joseperez@midominio.net
```

76.5.4. Opción http_port.

Esta opción es utilizado para indicar el puerto a través del cual escuchará peticiones Squid. EL valor predeterminado es 3128, es deicr, Squid escuchará peticiones a través del puerto 3128/tcp.

```
http_port 3128
```

El puerto estándar designado para servidores de caché de Internet (webcache) es el puerto 8080.

```
http_port 8080
```

La opción permite establecer también si se quiere utilizar una dirección IP en particular. Esto añade mayor seguridad al servicio, pues si se tiene dos tarjetas de red, una con una dirección IP pública y otra con una dirección IP privada, se puede establecer que Squid solo permita conexiones desde la dirección IP privada.

```
http_port 192.168.80.1:8080
```

Si se necesita configurar un servidor proxy en modo transparente, solo es necesario añadir la opción **intercept**, misma que desde la versión 3.1 de Squid reemplaza a la opción **transparent**.

```
http_port 192.168.80.1:8080 intercept
```

Nota.

Para configurar un servidor proxy en modo transparente en CentOS 5 y Red Hat EnterpriseLinux 5 y versiones anteriores, utilice la opción **transparent**:

```
http_port 192.168.80.1:8080 transparent
```

76.5.5. Opción cache_dir.

Esta opción se utiliza para establecer que tamaño se desea que utilice Squid para almacenamiento de caché en el disco duro. De modo predeterminado Squid utilizará el formato **ufs** para crear en el directorio **/var/spool/squid** un caché de 100 MB, dividido en jerarquías de 16 directorios subordinados, hasta 256 niveles cada uno:

```
cache_dir ufs /var/spool/squid 100 16 256
```

Se puede incrementar el tamaño del caché hasta donde lo desee el administrador. Mientras más grande sea el caché, más objetos se almacenarán en éste y por lo tanto se consumirá menos el ancho de banda. La siguiente línea establece un caché de 2 GB:

```
cache_dir ufs /var/spool/squid 2048 16 256
```

El formato de cache **ufs** puede llegar a bloquear el proceso principal de Squid en operaciones de entrada/salida sobre el sistema de archivos cuando hay muchos clientes conectados. Para evitar que esto ocurra, se recomienda utilizar **aufs**, que utiliza el mismo formato de **ufs**, pero funciona de manera *asincrónica*, consiguiéndose un mejor desempeño.

```
cache_dir aufs /var/spool/squid 2048 16 256
```

76.5.6. Opción maximum_object_size.

Esta opción se utiliza para definir el tamaño máximo de los objetos en el caché. Se recomienda establecerla en escenarios con alta carga de trabajo, puesto que permite evitar desperdiciar recursos de sistema almacenando en el caché objetos de gran tamaño que probablemente sólo sean aprovechados por unos pocos usuarios, optimizando el uso del caché con objetos pequeños que de otro modo generarían una gran cantidad de peticiones hacia las redes públicas. En el siguiente ejemplo se establece un límite de 48 MB para los objetos del caché.

```
maximum_object_size 48 MB
```

76.5.7. Opciones cache_swap_low y cache_swap_high.

Es posible realizar una limpieza automática del caché de Squid cuando éste llegue a cierta capacidad. La opción **cache_swap_low** establece el porcentaje a partir del cual se comenzará a limpiar el cache. La opción **cache_swap_high** establece el porcentaje a partir del cual se comenzará a limpiar de manera agresiva el cache. En el siguiente ejemplo se establece que el cache se comienza a limpiar cuando alcanza el 90% y se comienza a limpiar de manera agresiva cuando alcanza el 95%.

```
cache_swap_low 90
cache_swap_high 95
```

Lo anterior permite tener un caché *saludable* que se limpia automáticamente. Se recomienda utilizar estas opciones en escenarios con alta carga de trabajo.

76.5.8. Opción cache_replacement_policy.

A través de esta opción se incluye soporte para los siguientes algoritmos para el caché:

LRU	Acrónimo de **L**east **R**ecently **U**sed, que traduce como **Menos Recientemente Utilizado**. En este algoritmo los objetos que fueron accedidos hace mucho tiempo, son eliminados primero y manteniendo siempre en el caché a los objetos más recientemente solicitados. **Ésta política es la utilizada por Squid de modo predeterminado**.
LFUDA	Acrónimo de **L**east **F**requently **U**sed with **D**ynamic **A**ging, que se traduce como **Menos Frecuentemente Utilizado con Envejecimiento Dinámico**. En este algoritmo los objetos más solicitados permanecen en el caché sin importar su tamaño optimizando la **eficiencia** (hit rate) por **octetos** (Bytes) a expensas de la eficiencia misma, de modo que un objeto grande que se solicite con mayor frecuencia impedirá que se pueda hacer caché de objetos pequeños que se soliciten con menor frecuencia.
GDSF	Acrónimo de **G**reedy**D**ual **S**ize **F**requency, que se traduce como **Frecuencia de tamaño *GreedyDual*** (*codicioso dual*), que es el algoritmo sobre el cual se basa **GDSF**. Optimiza la **eficiencia** (hit rate) por objeto manteniendo en el caché los objetos pequeños más frecuentemente solicitados de modo que hay mejores posibilidades de lograr **respuesta a una solicitud** (hit). Tiene una eficiencia por **octetos** (Bytes) menor que el algoritmo **LFUDA** debido a que descarta del caché objetos grandes que sean solicitado con frecuencia.

El algoritmo recomendado y que ha demostrado mejor desempeño en escenarios de alta carga de trabajo es LFUDA.

```
cache_replacement_policy heap LFUDA
```

76.5.9. Opción cache_mem.

La opción **cache_mem** establece la cantidad ideal de memoria para lo siguiente:

- Objetos en tránsito.
- Objetos frecuentemente utilizados (*Hot*).
- Objetos negativamente almacenados en el caché.

Los datos de estos objetos se almacenan en bloques de 4 Kb. La opción **cache_mem** especifica un límite máximo en el tamaño total de bloques acomodados, donde los objetos en tránsito tienen mayor prioridad. Sin embargo los objetos frecuentemente utilizados (*Hot*) y aquellos negativamente almacenados en el caché, podrán utilizar la memoria sin utilizar hasta que esta sea requerida. De ser necesario, si un objeto en tránsito es mayor a la cantidad de memoria especificada, **Squid** excederá lo que sea necesario para satisfacer la petición.

De modo predeterminado, desde la versión 3.1 de Squid, se establecen 256 MB, que es más que suficiente para las necesidades de redes de área local con pocos anfitriones. Puede especificar una cantidad menor para obtener un mejor rendimiento, pues conviene utilizar la memoria disponible para hacer cache en memoria de muchos objetos pequeños que son frecuentemente visitados, que hacer cache de unos pocos objetos grandes que sólo unos pocos usuarios aprovecharán. En el siguiente ejemplo se establecen 48 MB como límite de tamaño para los objetos en tránsito:

```
cache_mem 48 MB
```

Nota.

En CentOS 5 y Red Hat EnterpriseLinux 5 y versiones anteriores, el valor predeterminado de **cache_mem** son 8 MB, por lo cual puede incrementar este valor hasta donde se considere pertinente.

```
cache_mem 32 MB
```

76.6. Estableciendo el idioma de los mensajes mostrados por Squid hacia el usuario.

Squid incluye traducción a distintos idiomas de las distintas páginas de error e informativas que son desplegadas en un momento dado durante su operación. Dichas traducciones se pueden encontrar en **/usr/share/squid/errors/**. Desde la versión 3.0 de Squid, el idioma se detecta automáticamente a partir del navegador utilizado por el usuario. Es innecesario modificar opción alguno, salvo que se haya personalizado los mensajes, en cuyo caso conviene utilizar una ruta distinta a la del idioma utilizado para evitar se sobre-escriban los archivos después de actualizar el sistema.

Nota.

En CentOS 5 y Red Hat™ Enterprise Linux 5 y versiones anteriores, el idioma de los mensajes de error se establece a través dla opción **error_directory**, cuyo valor predeterminado es **/usr/share/squid/errors/English** y puede ser cambiado por el valor **/usr/share/squid/errors/Spanish**:

```
error_directory /usr/share/squid/errors/Spanish
```

76.7. Iniciando, reiniciando y añadiendo el servicio al arranque del sistema.

Una vez terminada la configuración, para iniciar por primera vez **Squid** ejecute:

```
service squid start
```

Si necesita volver a cargar la configuración para probar cambios realizados, sin detener el servicio, ejecute:

```
service squid reload
```

Si necesita reiniciar para probar cambios hechos en la configuración, considerando que este proceso puede llegar a demorar algunos minutos, ejecute:

```
service squid restart
```

Para que **Squid** inicie de manera automática junto con el sistema, ejecute:

```
chkconfig squid on
```

Lo anterior habilitará el servicio **squid** en todos los niveles de ejecución.

76.8. Depuración de errores

Cualquier error al inicio de **Squid** sólo significa que hubo errores de sintaxis, errores de dedo o bien se están citando incorrectamente las rutas hacia los archivos de las **Listas de Control de Acceso**.

Puede realizar diagnóstico de problemas indicándole a **Squid** que vuelva a leer configuración, lo cual devolverá los errores que existan en el archivo **/etc/squid/squid.conf**.

```
service squid reload
```

Cuando se trata de errores graves que impiden iniciar el servicio, puede examinarse el contenido del archivo **/var/log/squid/squid.out** con el mandato **less**, **more** o cualquier otro visor de texto:

```
tail -80 /var/log/squid/squid.out
```

76.9. Modificaciones necesarias en el muro cortafuegos.

Si se utiliza un cortafuegos con políticas estrictas, como por ejemplo **Shorewall**, es necesario abrir el puerto 8080 por TCP (**webcache**), si se eligió utilizar el puerto 8080 en lugar del 3128.

La regla para el archivo **/etc/shorewall/rules** de **Shorewall**, que sólo permitirá el acceso hacia **Squid** desde la zona de red de área local, correspondería a algo similar a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  loc     fw      tcp     8080
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Para aplicar los cambios en Shorewall, ejecute:

```
service shorewall restart
```

76.9.1. Re-direccionamiento de peticiones a través de la opción REDIRECT en Shorewall.

La acción **REDIRECT** en **Shorewall** permite redirigir peticiones hacia protocolo **HTTP** para hacerlas pasar a través de **Squid**. En el siguiente ejemplo las peticiones hechas desde la zona que corresponde a la red local serán redirigidas hacia el puerto 8080 del cortafuegos, en donde está configurado **Squid** configurado como **Servidor Proxy** (Proxy) transparente.

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  loc     fw      tcp     8080
REDIRECT        loc     8080    tcp     80
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

76.9.1.1. Exclusión de sitios en Shorewall.

En el caso de sitios que se quiera excluir de ser utilizados con Squid, es decir, sitios problemáticos, se puede configurar en Shorewall que el acceso sea directo, con una configuración similar a la del siguiente ejemplo, donde se excluye de pasar por Squid las peticiones dirigidas a las redes 201.144.108.0/24 (IMSS.gob.mx) y 200.33.74.0/24 (SAT.gob.mx) y se abre el paso directo desde la red local hacia esta red:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  loc     fw      tcp     8080
REDIRECT        loc     8080                    tcp     80      -       !201.144.108.0/24,200.33.74.0/24
ACCEPT          loc     net:201.144.108.0/24    all
ACCEPT          loc     net:200.33.74.0/24      all
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

76.9.2. Re-direccionamiento de peticiones a través de iptables.

Bajo ciertas circunstancias, se requerirá tener salida transparente hacia Internet para ciertos servicios, pero al mismo tiempo se necesitará re-direccionar peticiones hacia servicio **HTTP** para pasar a través del el puerto donde escucha peticiones **Squid**, como proxy en modo *transparente*, es decir el puerto 8080/tcp, de modo que se impida la salida hacia alguna hacia servidores **HTTP** en el exterior sin que ésta pase antes por **Squid**. Ningún **proxy** conocido puede funcionar en modo *transparente* para los protocolos **HTTPS**, **FTP**, **GOPHER** ni **WAIS**, por lo que dichos protocolos tendrán que ser filtrados a través del **NAT**.

El re-direccionamiento se hace a través de **iptables**. Considerando para este ejemplo que la red local se accede a través de una interfaz eth1, el siguiente esquema ejemplifica un re-direccionamiento:

```
iptables -A INPUT -m state --state NEW -m tcp -p tcp \
     -i eth1 --dport 8080 -j ACCEPT
iptables -t nat -A PREROUTING -i eth1 -p tcp \
    --dport 80 -j REDIRECT --to-port 8080
service iptables save
```

77. Configuración de Squid: Acceso por autenticación

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

77.1. Introducción.

Es muy útil el poder establecer un sistema de autenticación para poder acceder hacia Internet, pues esto permite controlar quienes si y quienes no accederán a Internet sin importar desde que máquina de la red local lo hagan. Sera de modo tal que tendremos un doble control, primero por dirección IP y segundo por nombre de usuario y contraseña.

Este documento considera que se ha leído previamente, a detalle y en su totalidad el documento titulado «Configuración de Squid: Servidor Proxy,» y que ha configurado exitosamente Squid como servidor proxy.

77.2. Equipamiento lógico necesario.

Para poder llevar la cabo los procedimientos descritos en este manual y documentos relacionados, se necesitará tener instalado al menos lo siguiente:

- squid-2.5.STABLE3
- httpd-2.0.x (Apache) (opcional)
- openldap-servers-2.2.x (opcional)

Eligiendo el módulo de autenticación.

Este manual considera poder autenticar a través de un archivo de texto simple con contraseñas creadas con htpasswd o bien a través de un servidor LDAP (una solución más robusta).

77.2.1. Autenticación a través del módulo LDAP.

Considerando que se ha configurado exitosamente OpenLDAP como servidor de autenticación, sólo se necesita definir el directorio (o subdirectorio) y el servidor LDAP a utilizar.

La sintaxis utilizada para squid_ldap_auth es la siguiente:

```
squid_ldap_auth -b "Directorio-a-utilizar" servidor-ldap-a-utilizar
```

Ejemplo:

```
squid_ldap_auth -b "ou=People,dc=dominio,dc=tld" 127.0.0.1
```

Edite el archivo /etc/squid/squid.conf:

```
vim /etc/squid/squid.conf
```

Añada la siguiente configuración, misma que considera que *squid_ldap_auth* se localiza en */usr/lib/squid/ncsa_auth*:

```
auth_param basic program /usr/lib/squid/squid_ldap_auth -b  "ou=People,dc=dominio,dc=tld" 127.0.0.1
```

Lo anterior conecta al directorio dc=su-red-local,dc=tld en el servidor LDAP en 127.0.0.1.

77.2.2. Autenticación a través del módulo NCSA

Squid puede utilizar el módulo *ncsa_auth*, de la NCSA (National Center for Supercomputing Applications) y que ya viene incluido como parte del paquete principal de Squid en la mayoría de las distribuciones actuales. Este módulo provee una autenticación muy sencilla a través de un archivo de texto simple cuyas contraseñas fueron creadas con htpasswd.

77.2.2.1. Creación del archivo de contraseñas.

Se requerirá la creación previa de un archivo que contendrá los nombres de usuarios y sus correspondientes contraseñas (cifradas). El archivo puede localizarse en cualquier lugar del sistema, con la única condición que sea asequible para el usuario *squid*.

Debe procederse a crear un archivo */etc/squid/claves*:

```
touch /etc/squid/claves
```

Salvo que vaya a utilizarse un guión a través del servidor web para administrar las contraseñas, como medida de seguridad, este archivo debe tener atributos de lectura y escritura sólo para el usuario *squid*:

```
chmod 600 /etc/squid/claves
chown squid:squid /etc/squid/claves
```

A continuación deberemos dar de alta las cuentas que sean necesarias, utilizando el mandato *htpasswd -mismo que viene incluido en el paquete httpd-2.0.x-*. Ejemplo:

```
htpasswd /etc/squid/claves joseperez
```

Lo anterior solicitará teclear una nueva contraseña para el usuario *joseperez* y confirmar tecleando ésta de nuevo. Repita con el resto de las cuentas que requiera dar de alta.

Todas las cuentas que se den de alta de este modo son independientes a las ya existentes en el sistema. Al dar de alta una cuenta o cambiar una contraseña lo estará haciendo **EXCLUSIVAMENTE** para el acceso al servidor Proxy. Las cuentas son independientes a las que se tengan existentes en el sistema como serían *shell*, correo y Samba.

Edite el archivo /etc/squid/squid.conf:

```
vim /etc/squid/squid.conf
```

Lo siguiente será especificar que programa de autenticación se utilizará. Localice la sección que corresponde a la etiqueta *auth_param basic program*. De modo predeterminado esta opción viene desactivada y carece de valores. Considerando que *ncsa_auth* se localiza en */usr/lib/squid/ncsa_auth*, se a añade lo siguiente:

```
auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/claves
```

/usr/lib/squid/ncsa_auth corresponde a la localización de el programa para autenticar y especificando como argumento el archivo*/etc/squid/claves*, el cual corresponde al que contiene los nombres de usuario y sus respectivas contraseñas.

77.3. Listas y reglas de control de acceso.

se debe especificar una lista de control de acceso denominada *passwd* la cual se configurará para utilizar de modo obligatorio la autenticación para poder acceder a Squid. Debe localizarse la sección de *Listas de Control de Acceso* y añadirse la siguiente línea:

```
acl password proxy_auth REQUIRED
```

Habiendo hecho lo anterior, debe haber algo similar a lo siguiente en la sección de *Listas de Control de Acceso*:

```
#
# Recommended minimum configuration:
acl all src 0.0.0.0/0
acl manager proto cache_object
acl localhost src 127.0.0.1/8

acl localnet src 192.168.1.0/24
acl password proxy_auth REQUIRED
```

Se procede entonces a modificar la regla de control de accesos que ya se tenía para permitir el acceso a Internet. Donde antes estaba lo siguiente:

```
http_access allow localnet
```

Se añade *passwd*, la definición de la *Lista de Control de Acceso* que requiere utilizar contraseña a la regla actual, de modo que quede como se muestra a continuación:

```
http_access allow localnet password
```

Habiendo hecho lo anterior, la zona de reglas de control de acceso debería quedar del siguiente modo:

```
#
# INSERT YOUR OWN RULE(S) HERE TO allow ACCESS FROM YOUR CLIENTS
#
http_access allow localhost
http_access allow localnet password

http_access deny all
```

77.3.1. Finalizando procedimiento.

Finalmente, sólo bastará recargar la configuración de Squid para que tomen efecto los cambios y se puedan realizar pruebas.

```
service squid reload
```

78. Configuración de Squid: Restricción de acceso a Sitios de Internet.

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

78.1. Introducción.

Denegar el acceso a ciertos Sitios de Red permite hacer un uso más racional del ancho de banda con el que se dispone. El funcionamiento es verdaderamente simple y consiste en denegar el acceso a nombres de dominio o direcciones de Internet que contengan patrones en común.

Este documento considera que se ha leído previamente, a detalle y en su totalidad el documento titulado «Configuración de Squid: Servidor Proxy,» y que ha configurado exitosamente Squid como servidor proxy.

78.2. Restricción por expresiones regulares.

Se debe crear un archivo donde se definirá la lista de expresiones regulares.

```
vim /etc/squid/listas/expreg-denegadas
```

Esta lista puede contener cualquier expresión regular que se considere sea usualmente utilizadas en las direcciones de ciertos sitios.

```
adult
celebri
mp3
otrositioindeseable.com
playstation
porn
sex
sitioindeseable.com
taringa
torrent
warez
wii
```

Esta lista, la cual deberá ser completada con todas las palabras (muchas de estás son palabras obscenas en distintos idiomas) y direcciones de Internet que el administrador considere pertinentes, la guardaremos como */etc/squid/listas/expreg-denegadas*.

Edite el archivo /etc/squid/squid.conf:

```
vim /etc/squid/squid.conf
```

Añada una lista de control, denominada expreg-denegadas, de acceso tipo url_regex (expresiones regulares del URL), que defina al la lista en el archivo /etc/squid/listas/expreg-denegadas:

```
acl expreg-denegadas url_regex "/etc/squid/listas/expreg-denegadas"
```

Habiendo hecho lo anterior, deberemos tener en la sección de *Listas de Control de Acceso* algo similar a lo siguiente:

```
#
# Recommended minimum configuration:
acl all src 0.0.0.0/0
acl manager proto cache_object
acl localhost src 127.0.0.1/8
acl localnet src 192.168.1.0/24
acl password proxy_auth REQUIRED
acl expreg-denegadas url_regex "/etc/squid/listas/expreg-denegadas"
```

A continuación especificaremos modificaremos una *Regla de Control de Acceso* existente agregando con un símbolo de *!* que se denegará el acceso a la *Lista de Control de Acceso* denominada *expreg-denegadas*:

```
http_access allow localnet !expreg-denegadas
```

La regla anterior permite el acceso a la *Lista de Control de Acceso* denominada *localnet*, pero le niega el acceso a todo lo que coincida con lo especificado en la *Lista de Control de Acceso* denominada *expreg-denegadas*.

Ejemplo aplicado a una *Regla de Control de Acceso* combinando el método de autenticación explicado en el documento Configuración de Squid: Acceso por Autenticación:

Reglas de control de acceso: denegación de sitios.

```
#
# INSERT YOUR OWN RULE(S) HERE TO allow ACCESS FROM YOUR CLIENTS
#
http_access allow localhost
http_access allow localnet password !expreg-denegadas
http_access deny all
```

78.3. Restricción por expresiones regulares.

Para restringir el acceso por dominios, se crea un archivo con lista con dominios.

```
vim /etc/squid/listas/dominios-denegados
```

Los nombres pueden ser nombres de dominio específicos:

```
www.facebook.com
www.twitter.com
plus.google.com
```

O bien puede definirse todo el dominio completo, incluyendo sub-dominios:

```
.facebook.com
.twitter.com
```

Nota.

Si define .dominio.com, es innecesario definir www.dominio.com o mail.dominio.com o ftp.dominio.com, etc., pues todos son subdominios de .dominio.com:

O bien se pueden definir dominios de nivel superior genéricos o geográficos.

```
.co.jp
.com.cn
.im
.tv
.xxx
```

O bien una combinación de todo lo anterior.

```
.co.jp
.com.cn
.facebook.com
plus.gogle.com
.tv
.twitter.com.im
.xxx
```

Edite el archivo /etc/squid/squid.conf.

```
vim /etc/squid/squid.conf
```

Añada una lista de control, denominada dominios-denegados, de acceso tipo dstdomain (dominios de destino), que defina al la lista en el archivo /etc/squid/listas/dominios-denegados.

```
acl dominios-denegados dstdomain "/etc/squid/listas/dominios-denegados"
```

Añada una regla de control de acceso que deniegue el acceso a sitios que estén incluidos en la lista de dominios.

```
http_access allow localnet !expreg-denegadas !dominios-denegados
```

78.3.1. Permitiendo acceso a sitios inocentes incidentalmente bloqueados.

Si por ejemplo, el incluir una expresión regular en particular, en la lista de expresiones regulares denegadas, afecta incidentalmente el acceso a un sitio de Internet en particular, también puede generarse una lista de dominios que serán excluidos de las restricciones.

Utilice el editor de texto para crear el archivo /etc/squid/dominios-inocentes.

```
vim /etc/squid/dominios-inocentes
```

El contenido puede ser una lista de dominios o bien dominios de nivel superior, que se considere deban ser accedidos por la red local en cualqueir momento y sin restricciones.

```
.alcancelibre.org
.edu
.edu.mx
.eluniversal.com.mx
.gob.mx
.gov
.milenio.com
.org
.org.mx
.unam.mx
www.google.com
www.google.com.mx
```

Este archivo será definido en una *Lista de Control de Acceso* del mismo modo en que se hizo anteriormente con el archivo que contiene dominios y palabras denegadas.

```
acl dominios-inocentes dstdomain "/etc/squid/dominios-inocentes"
```

Para hacer uso de el archivo, sólo bastará utilizar la expresión **!** en la misma línea utilizada para la *Regla de Control de Acceso* establecida para denegar el mismo.

```
http_access allow all dominios-inocentes
```

La regla anterior especifica que se permitirá el libre acceso, en todo momento, a los dominios incluidos en la lista de control de acceso denominada *dominios-inocentes*.

78.3.2. Finalizando procedimiento.

Finalmente, sólo bastará recargar la configuración de Squid para que tomen efecto los cambios y se puedan realizar pruebas.

```
service squid reload
```

79. Configuración de Squid: Restricción de acceso a contenido por extensión.

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

79.1. Introducción.

Denegar el acceso a ciertos tipos de extensiones de archivo permite hacer un uso más racional del ancho de banda con el que se dispone. El funcionamiento es verdaderamente simple y consiste en denegar el acceso a ciertos tipos de extensiones que coincidan con lo establecido en una *Lista de Control de Acceso*.

Este documento considera que se ha leído previamente, a detalle y en su totalidad el documento titulado «Configuración de Squid: Servidor Proxy,» y que ha configurado exitosamente Squid como servidor proxy.

79.2. Definiendo elementos de la Lista de Control de Acceso.

Lo primero será generar una lista la cual contendrá direcciones de Internet y palabras usualmente utilizadas en nombres de ciertos dominios. Ejemplos:

```
\.avi$
\.mp4$
\.mp3$
\.mp4$
\.mpg$
\.mpeg$
\.mov$
\.ra$
\.ram$
\.rm$
\.rpm$
\.vob$
\.wma$
\.wmv$
\.wav$
\.doc$
\.xls$
\.mbd$
\.ppt$
\.pps$
\.ace$
\.bat$
\.exe$
\.lnk$
\.pif$
\.scr$
\.sys$
\.zip$
\.rar$
```

Esta lista, la cual deberá ser completada con todas las extensiones de archivo que el administrador considere pertinentes, la guardaremos como */etc/squid/listas/extensiones*.

Edite el archivo /etc/squid/squid.conf:

```
vim /etc/squid/squid.conf
```

Se debe definir una *Lista de Control de Acceso* que a su vez defina al archivo */etc/squid/listas/extensiones*. Esta lista la denominaremos como "*extensiones*". De modo tal, la línea correspondiente quedaría del siguiente modo:

```
acl extensiones urlpath_regex "/etc/squid/listas/extensiones"
```

Habiendo hecho lo anterior, se debe añadir en la sección de *Listas de Control de Acceso* algo similar a lo siguiente:

```
#
# Recommended minimum configuration:
acl all src 0.0.0.0/0

acl manager proto cache_object
acl localhost src 127.0.0.1/8
acl localnet src 192.168.1.0/24
acl password proxy_auth REQUIRED

acl expregs url_regex "/etc/squid/listas/expregs"
acl extensiones urlpath_regex "/etc/squid/listas/extensiones"
```

A continuación especificaremos modificaremos una *Regla de Control de Acceso* existente agregando con un símbolo de *!* que se denegará el acceso a la *Lista de Control de Acceso* denominada *extensiones*:

```
http_access allow localnet !extensiones
```

La regla anterior permite el acceso a la *Lista de Control de Acceso* denominada *localnet*, pero le niega el acceso a todo lo que coincida con lo especificado en la *Lista de Control de Acceso* denominada *extensiones*.

Ejemplo aplicado a una *Regla de Control de Acceso* combinando el método de autenticación explicado en el documento Cómo configurar Squid: Acceso por Autenticación y el de denegación hacia Sitio de Red explicado en el documento Cómo configurar Squid: Restricción de acceso a Sitio de Red:

Reglas de control de acceso: denegación de extensiones.

```
#
# INSERT YOUR OWN RULE(S) HERE TO allow ACCESS FROM YOUR CLIENTS
#
http_access allow localhost

http_access allow localnet password !expregs !extensiones
http_access deny all
```

79.2.1. Finalizando procedimiento.

Finalmente, sólo bastará recargar la configuración de Squid para que tomen efecto los cambios y se puedan realizar pruebas.

```
service squid reload
```

80. Configuración de Squid: Restricción de acceso por horarios.

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

80.1. Introducción.

Denegar el acceso a ciertos en ciertos horarios permite hacer un uso más racional del ancho de banda con el que se dispone. El funcionamiento es verdaderamente simple y consiste en denegar el acceso en horarios y días de la semana.

Este documento considera que se ha leído previamente, a detalle y en su totalidad el documento titulado «Configuración de Squid: Servidor Proxy,» y que ha configurado exitosamente Squid como servidor proxy.

80.2. Procedimientos

Edite el archivo /etc/squid/squid.conf:

```
vim /etc/squid/squid.conf
```

La sintaxis para crear *Listas de control de acceso* que definan horarios, es la siguiente:

```
acl [nombre del horario] time [días de la semana] hh:mm-hh:mm
```

Los días de la semana se definen con letras, las cuales corresponden a la primera letra del nombre en inglé, de modo que se utilizarán del siguiente modo:

- **S** - Domingo
- **M** - Lunes
- **T** - Martes
- **W** - Miércoles
- **H** - Jueves
- **F** - Viernes
- **A** - Sábado

Ejemplo:

```
acl semana time MTWHF 09:00-21:00
```

Esta regla define a la lista *semana*, la cual comprende un horario de 09:00 a 21:00 horas desde el Lunes hasta el Viernes.

Este tipo de listas se aplican en las *Reglas de Control de Acceso* con una mecánica similar a la siguiente: se permite o deniega el acceso en el horario definido en la *Lista de Control de Acceso* denominada *X* para las entidades definidas en la *Lista de Control de Acceso* denominada *Y*. Lo anterior expresado en una *Regla de Control de Acceso*, quedaría del siguiente modo:

```
http_access [allow | deny] [nombre del horario] [lista de entidades]
```

Ejemplo: Se quiere establecer que los miembros de la *Lista de Control de Acceso* denominada *localnet* tengan permitido acceder hacia Internet en un horario que denominaremos como *matutino* y que comprende de lunes a viernes de 09:00 a 15:00 horas.

La defínción para le horario correspondería a:

```
acl localnet src 192.168.1.0/24
acl matutino time MTWHF 09:00-15:00
```

La definición de la *Regla de Control de Acceso* sería:

```
http_access allow matutino localnet
```

Lo anterior, en resumen, significa que quienes conformen *localnet* podrán acceder a Internet de Lunes a Viernes de 09:00-15:00 horas.

80.2.1. Más ejemplos.

80.2.1.1. Restringiendo el tipo de contenido.

es posible denegar acceso a cierto tipo de contenido de acuerdo a su extensión. Se requiere una *Lista de Control de Acceso* y una *Regla de Control de Acceso*

Si se necesita una lista denominada *extensiones* que defina a todos los archivos con extensión .mp3, utilizaríamos lo siguiente:

```
acl localnet src 192.168.1.0/24
acl extensiones urlpath_regex \.mp3$
```

Si queremos denegar el acceso al todo contenido con extensión .mp3, la regla quedaría del siguiente modo:

```
http_access allow localnet !extensiones
```

80.2.1.2. Combinando reglas de tiempo y contenido.

Si por ejemplo queremos restringir parcialmente el acceso a cierto tipo de contenido a ciertos horarios, pueden combinarse distintos tipos de reglas.

```
acl localnet src 192.168.1.0/24
acl matutino time MTWHF 09:00-15:00
acl extensiones urlpath_regex .mp3$
http_access allow matutino localnet !extensiones
```

La *Regla de Control de Acceso* anterior especifica **acceso permitido**, en el horario definido como *matutino*, a quienes integran la *Lista de Control de Acceso* denominada *localnet*, para acceder hacia todo tipo de contenido, **excepto** a los contenidos que coincidan con los definidos en la *Lista de Control de Acceso* denominada *extensiones*.

80.2.2. Finalizando procedimiento.

Finalmente, sólo bastará recargar la configuración de Squid para que tomen efecto los cambios y se puedan realizar pruebas.

```
service squid reload
```

81. Cómo configurar squid con soporte para direcciones MAC.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales (incluyendo su publicación, a través de cualquier medio, por entidades con fines de lucro). c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en castellano. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

81.1. Introducción.

81.1.1. Acerca de Squid.

Squid es un **Servidor Intermediario** (*Proxy*) de alto desempeño que se ha venido desarrollando desde hace varios años y es hoy en día un muy popular y ampliamente utilizado entre los sistemas operativos como GNU/Linux y derivados de Unix®. Es muy confiable, robusto y versátil y se distribuye bajo los términos de la Licencia Pública General GNU (**GNU/GPL**). Siendo equipamiento lógico **libre**, está disponible el código fuente para quien así lo requiera. de modo predeterminado no está incluido el soporte para listas de control de acceso basadas sobre direcciones **MAC** (**M**edia **A**ccess **C**ontrol).

81.2. Equipamiento lógico necesario.

81.2.1. Instalación a través de yum.

A partir de CentOS 5.6 y Red Hat Enterprise Linux 5.6, el paquete de Squid ya incluye soporte para direcciones MAC. Solo es necesario ejecutar lo siguiente:

```
yum -y install squid
```

81.3. Procedimientos

Este documento considera que se ha leído a detalle el documento «*Cómo configurar Squid: Parámetros básicos para servidor de intermediación (Proxy)*». Se requiere se hayan configurado al menos los siguientes parámetros:

- **http_port**, ejemplo: `http_port 8080 transparent`
- **cache_dir**, ejemplo: `cache_dir ufs /var/spool/squid 1024 16 256`
- **error_directory**, ejemplo: `error_directory /usr/share/squid/errors/Spanish`

Se requiere además determinar los valores las siguientes variables que deberán ser reemplazadas por datos reales:

- Las direcciones **MAC** especificadas en los ejemplos.

- las direcciones **MAC** de todos los equipos de la **LAN** se pueden obtener, si se está realizando las operaciones desde un servidor que sirve de puerta de enlace, utilizando el mandato **arp** con la opción -**n**, es decir: **arp -n**.

- Alternativamente, la dirección **MAC** desde una estación trabajo con Windows se puede obtener la dirección **MAC** utilizando el mandato **ipconfig** con la opción /**all**: `ipconfig /all`

- Alternativamente, la dirección **MAC** desde una estación trabajo con Linux se puede obtener la dirección **MAC** utilizando el mandato **ifconfig**.

Archivo /etc/squid/listas/macsredlocal.

Crear un archivo denominado /**etc/squid/listas/macsredlocal**

```
vi /etc/squid/listas/macsredlocal
```

Donde el contenido será una lista de direcciones **MAC** a la cual se aplicarán reglas de control de acceso. Ejemplo:

```
00:01:80:41:9C:8A
00:08:A1:84:18:AD
00:16:E3:9D:CD:77
00:04:75:AA:2D:A1
00:19:D2:6B:41:45
00:13:10:8D:4A:EE
00:19:21:14:9B:0D
```

81.3.1. Archivo /etc/squid/squid.conf

Se edita el archivo /**etc/squid/squid.conf**:

```
vi /etc/squid/squid.conf
```

En éste se debe configurar la lista de control de acceso con un nombre que la identifique y diferencie claramente de las demás listas, asignado el tipo de lista como **arp**. En el siguiente ejemplo, se crea la lista de control de acceso denominada **macsredlocal** de tipo **arp** y cuyos elementos que la conforman están en el archivo /**etc/squid/listas/macsredlocal**:

```
acl macsredlocal arp "/etc/squid/listas/macsredlocal"
```

Se crea una regla de control de acceso que permita a los miembros de la lista de control de acceso hacer algo. En el siguiente ejemplo se define que está permitido el acceso a la lista **macsredlocal**:

```
http_access allow macsredlocal
```

Si se creo alguna lista para limitar el acceso hacia palabras y otra para extensiones, como se describe en los documentos «*Cómo configurar Squid: Restricción de acceso a Sitios de Red*» y «*Cómo configurar Squid: Restricción de acceso a contenido por extensión*», la regla de control de acceso podría quedar de la siguiente manera:

```
http_access allow macsredlocal !porno !extensiones
```

Si además se creo alguna lista para limitar los horarios de acceso, como se describe en el documento «*Cómo configurar Squid: Restricción de acceso por horarios*», la regla de control de acceso podría quedar de la siguiente manera:

```
http_access allow matutino macsredlocal !porno !extensiones
```

Cualquier otra forma de utilizar la lista de control de acceso con direcciones **MAC** dependerá de la imaginación del administrador.

81.4. Iniciar, detener y reiniciar el servicio squid.

Para ejecutar por primera vez el servicio **squid** con las configuraciones creadas, utilice:

```
service squid start
```

Para hacer que los cambios hechos tras modificar la configuración surtan efecto, utilice:

```
service squid restart
```

Para detener el servicio **squid** utilice:

```
service squid stop
```

Para hacer que el servicio de **squid** esté activo con el siguiente inicio del sistema, en todos los niveles de ejecución (2, 3, 4 y 5), se utiliza lo siguiente:

```
chkconfig squid on
```

82. Configuración de Squid: Cachés en jerarquía.

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

82.1. Introducción.

Colocar cachés en jerarquía en redes grandes donde hay múltiples servidores proxy, ayuda a ahorrar y aprovechar mejor los recursos.

82.1.1. Procedimientos

El parámetro cache_peer se utiliza para especificar otros **Servidores Proxy** con caché en una jerarquía como **padres** o como **hermanos**. Es decir, definir si hay un **Servidor Intermediario** adelante o en paralelo. La sintaxis básica es la siguiente:

```
cache_peer servidor tipo http_port icp_port opciones
```

Edite el archivo **/etc/squid/squid.conf**:

```
vim /etc/squid/squid.conf
```

Si el caché va a estar trabajando detrás de otro servidor cache, es decir un caché padre y considerando que el caché padre tiene una IP 172.16.100.1, escuchando peticiones **HTTP** en el puerto 8080 y peticiones ICP en puerto 3130 **(puerto utilizado de modo predeterminado por Squid)**, especificando que se omita almacenar en caché los objetos que ya están presentes en el caché del **Servidor Intermediario** padre, utilice la siguiente línea:

```
cache_peer 172.16.100.1 parent 8080 3130 proxy-only
```

Cuando se trabaja en redes muy grandes donde existen varios Servidores Intermediarios (Proxy) haciendo caché de contenido de Internet, es una buena idea hacer trabajar todos los caché entre si. Configurar caches vecinos como **sibling** (hermanos) tiene como beneficio el que se consultarán estos caches localizados en la red local antes de acceder hacia Internet y consumir ancho de banda para acceder hacia un objeto que ya podría estar presente en otro caché vecino.

Ejemplo: Si el caché va a estar trabajando en paralelo junto con otros caches, es decir caches hermanos y considerando los caches tienen IP 10.1.0.1, 10.2.0.1 y 10.3.0.1, todos escuchando peticiones **HTTP** en el puerto 8080 y peticiones ICP en puerto 3130, especificando que se omitirá se almacenen en caché los objetos que ya están presentes en los caches hermanos, utilice las siguientes líneas:

```
cache_peer 10.1.0.1 sibling 8080 3130 proxy-only
cache_peer 10.2.0.1 sibling 8080 3130 proxy-only
cache_peer 10.3.0.1 sibling 8080 3130 proxy-only
```

Pueden hacerse combinaciones que de manera tal que se podrían tener caches padres y hermanos trabajando en conjunto en una red local. Ejemplo:

```
cache_peer 10.0.0.1 parent 8080 3130 proxy-only
cache_peer 10.1.0.1 sibling 8080 3130 proxy-only
cache_peer 10.2.0.1 sibling 8080 3130 proxy-only
cache_peer 10.3.0.1 sibling 8080 3130 proxy-only
```

En los casos anteriores, la resolución de nombres se hace de manera local. Si se desea hacer que la resolución de nombres se realice en el servidor padre, se puede utilizar algo similar a lo siguiente:

```
cache_peer 10.0.0.1 parent 8080 3130 no-query no-digest default
```

Para aplicar los cambios en Squid, ejecute:

```
service squid reload
```

83. Configuración de WPAD

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

83.1. Introducción.

Gracias a que una gran cantidad de sitios de Internet ahora funcionan a través de HTTPS, resulta poco práctico configurar servidores intermediarios (proxies) en modo transparente, pues éstos solo permiten el modo transparente para el protocolo HTTP (puerto 80/TCP), obligando a los administradores de redes de área local a configurar la salida del protocolo HTTPS (puerto 443/TCP) a través de NAT en el muro cortafuegos.

Una forma de enfrentar el problema y poder controlar y filtrar la actividad de los usuarios a través de HTTPS, es olvidarse del modo transparente de Squid y utilizar una configuración manual del servidor proxy. Sin embargo, ésto representaría una enorme cantidad de trabajo para los administradores de redes de área local, quienes tendrían que pasar anfitrión por anfitrión a realizar la configuración. Ésta, sin embargo, se puede automatizar anunciando ésta a través de servidores DHCP y servidores DNS, utilizando **WPAD**.

Eliminar la configuración de proxy en modo trasparente y utilizar en su lugar el método descrito en este documento, combinado con una configuración del proxy-cache que permita el acceso hacia Internet utilizando sólo a una lista blanca y el cierre de la salida por NAT hacia el puerto 443, además de permitir **bloquear** servicios como **Facebook**, permite también **bloquear** de manera eficiente programas como **Ultrasurf** y **Your Freedom**.

83.1.1. Acerca de WPAD.

WPAD (**W**eb **P**roxy **A**uto-**D**iscovery protocol) es un método utilizado por los clientes de servidores Proxy para localizar el URI de un archivo de configuración, valiéndose de métodos de descubrimiento a través de DHCP y DNS.

Los clientes descargan y ejecutan un archivo, que debe denominarse **wpad.dat**, utilizando el formato de auto-configuración de proxy (**PAC**, **P**roxy **A**uto-**C**onfig) diseñado por Netscape en 1996 para Netscape Navigator 2.0.

El **borrador** del protocolo **WPAD**, el cual expiró en 1999, fue elaborado por un consorcio de empresas que incluían a Inktomi Corp., Microsoft, Real Networks Inc. y Sun Microsystems Inc. A pesar de tratarse de un **borrador que ha expirado**, la mayoría de los navegadores modernos incluyen soporte para este protocolo.

83.2. Procedimientos.

Este documento asume que se tiene configurado un servidor proxy-cache con Squid, un servidor DHCP y un servidor DNS. Por favor, cambie todos los valores **resaltados** en el procedimiento por aquellos que correspondan al escenario de su red de área local.

83.2.1. Equipamiento lógico necesario.

Instale Apache en el servidor que utilice como muro cortafuegos/proxy.

```
yum -y install httpd
```

Inicie el servicio **httpd**.

```
service httpd start
```

Para que el servicio **httpd** inicie junto con el sistema, ejecute lo siguiente:

```
chkconfig httpd on
```

83.2.2. Ajustes en el muro cortafuegos.

Es necesario abrir en el muro cortafuegos el puerto 80 por TCP (**HTTP**) para la red de área local. Se asume que ya están abiertos los puertos correspondientes al resto de los servicios involucrados, es decir los puertos 67 (bootps), 68 (bootpc) y 53 (domain) por TCP y UDP.

83.2.2.1. Shorewall.

Edite el archivo el archivo **/etc/shorewall/rules**:

```
vim /etc/shorewall/rules
```

Elimine la configuración de *proxy transparente* deshabilitando las reglas correspondientes a la salida desde la zona correspondiente a la red de área local hacia los puertos 20 (ftp-data), 21 (ftp) y 443 (https) en la zona correspondiente a la red pública y la regla que redirige hacia el puerto 8080 (webcache) las peticiones desde la red de área local hacia el puerto 80 (http):

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
#ACCEPT loc     net     tcp     20,21,443
#REDIRECT       loc     8080    tcp     80
#
```

Asumiendo que Squid escucha peticiones en el puerto 8080 y que sólo se permitirán conexiones desde la red de área local, la regla que habilita el acceso desde la red de área local hacia los puertos 8080 (webcache) y 80 (http) del muro cortafuegos correspondería a algo similar a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
#ACCEPT loc     net     tcp     20,21,443
#REDIRECT       loc     8080    tcp     80
#
ACCEPT  loc     fw      tcp     80,8080
```

Para aplicar los cambios en Shorewall, ejecute lo siguiente:

```
service shorewall restart
```

83.2.2.2. Servicio iptables.

Asumiendo que Squid escucha peticiones en la puerto 8080 y que la red de área local corresponde a **172.16.1.0**/**28**, ejecute lo siguiente:

```
iptables -A INPUT -s 172.16.1.0/28 -m state --state NEW \
    -m tcp -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -s 172.16.1.0/28 -m state --state NEW \
    -m tcp -p tcp --dport 8080 -j ACCEPT
iptables -A FORWARD -p tcp --dport 20:21 -j DROP
iptables -A FORWARD -p tcp --dport 443 -j DROP
service iptables save
```

O bien edite el archivo **/etc/sysconfig/iptables**:

```
vim /etc/sysconfig/iptables
```

Y añada lo siguiente:

```
-A INPUT -s 172.16.1.0/28 -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A INPUT -s 172.16.1.0/28 -m state --state NEW -m tcp -p tcp --dport 8080 -j ACCEPT
-A FORWARD -p tcp --dport 20:21 -j DROP
-A FORWARD -p tcp --dport 443 -j DROP
```

Y reinicie el servicio **iptables**:

```
service iptables restart
```

83.2.3. Resolución local del nombre de anfitrión.

Edite el archivo **/etc/hosts**:

```
vim /etc/hosts
```

Asumiendo que la dirección IP del anfitrión es **172.16.1.1** y que el dominio de la red de área local es red-local.net, **añada** la siguiente línea **resaltada en negrita** y **respetando el resto del contenido existente en este archivo**:

```
127.0.0.1       localhost.localdomain   localhost
::1             localhost6.localdomain6 localhost6
172.16.1.1      servidor.red-local.net  servidor
172.16.1.1      wpad.red-local.net      wpad
```

Modifique lo que sea necesario para que ajuste a la configuración utilizada en su red de área local.

83.2.4. Archivo wpad.dat.

Genere el directorio **/var/www/wpad** con permisos de acceso y escritura para usuario y de acceso para grupo y otros (rwxr-xr-x):

```
mkdir -m 0755 /var/www/wpad
```

Cualquier error en la sintaxis hará que el archivo sea imposible de utilizar. Puede descargar un archivo plantilla desde AlcanceLibre.org ejecutando lo siguiente:

```
wget http://www.alcancelibre.org/linux/secrets/wpad.dat \
    -O /var/www/wpad/wpad.dat
```

Edite el archivo **/var/www/wpad/wpad.dat** y modifique lo que sea necesario para que ajuste a la configuración utilizada en su red de área local.

```
vim /var/www/wpad/wpad.dat
```

Asumiendo que la red de área local corresponde a **172.16.1.0/28** y que Squid está funcionando en el anfitrión **172.16.1.1**, escuchando peticiones en el puerto 8080, añada el siguiente contenido:

```
function FindProxyForURL(url, host)
{
        if (
            isInNet(host, "172.16.1.0",  "255.255.255.240")
        ||  isInNet(host, "127.0.0.0", "255.0.0.0")
        ||  shExpMatch(host, "172.16.1.*")
        ||  shExpMatch(host, "127.*" )
        ||  shExpMatch(host, "localhost")
        ||  shExpMatch(host, "*.red-local.net")
        ||  isPlainHostName(host)
        ||  dnsDomainIs(host, ".red-local.net")
        ) {
            return "DIRECT";
          }
        else
          {
            return "PROXY servidor.red-local.net:8080";
          }
}
```

Es indispensable que el archivo **/var/www/wpad/wpad.dat** tenga permisos de lectura para todos, de otro modo será imposible compartirlo a través del servicio **httpd**.

```
chmod a+r /var/www/wpad/wpad.dat
```

83.2.5. Configuración de Apache.

Genere el archivo **/etc/httpd/conf.d/wpad.conf**:

```
vim /etc/httpd/conf.d/wpad.conf
```

Añada el siguiente contenido:

```
NameVirtualHost *:80
<VirtualHost *:80>
        ServerName wpad.red-local.net
        ServerAlias wpad
        DocumentRoot /var/www/wpad
        ErrorLog logs/wpad-error_log
        CustomLog logs/wpad-access_log combined
        <Directory "/var/www/wpad">
                AddType application/x-ns-proxy-autoconfig .dat
                DirectoryIndex wpad.dat
                Order Deny,Allow
                Deny from all
                Allow from 127.0.0.0/8 172.16.1.0/28
   </Directory>
</VirtualHost>
```

Modifique lo que sea necesario para que ajuste a la configuración utilizada en su red de área local.

A fin de evitar problemas con algunos navegadores, **se recomienda que éste sea el único anfitrión virtual en el servidor** o cuando menos sea el anfitrión virtual predeterminado.

Recargue o reinicie el servicio **httpd**.

```
service httpd reload
```

83.2.6. Anuncio del archivo wpad.dat.

El anuncio del archivo wpad.dat sólo puede hacerse a través de **uno** de los dos siguientes métodos:

a. A través de un servidor DHCP.
b. A través de un servidor DNS.

Se puede utilizar indistintamente uno u otro método. **Jamás combine ambos métodos** porque los anuncios serían ignorados por los navegadores. El método más estándar es el anuncio a través de un servidor DHCP.

83.2.6.1. Anuncio a través de servidor DNS.

Se requiere configurar el servidor DNS para que incluya dos registros, uno que resuelva el nombre wpad.**red-local.net** y el otro que indique el URI del archivo wpad.dat.

Asumiendo que tiene configurado y funcionando un servidor DNS con una **zona estática** que resuelve los nombres de anfitrión y direcciones IP de la red de área local, edite el archivo de zona correspondiente:

```
vim /var/named/data/red-local.net.zone
```

Cambie el número de serie de la zona y añada los siguientes dos registros en la zona de reenvío en el DNS utilizado por la red de área local. En el ejemplo se asume que el servidor HTTP que hospeda al archivo wpad.dat corresponde a la dirección IP **172.16.1.1**:

```
wpad    IN      A       172.16.1.1
@       IN      TXT     "service: wpad:!http://wpad.red-local.net:80/wpad.dat"
```

Reinicie el servicio **named**.

```
service named restart
```

Si se trata de una **zona dinámica**, utilice el mandato **nsupdate** para conectarse al servidor DNS:

```
nsupdate -k /etc/rndc.key
```

Desde el intérprete de mandatos de **nsupdate**, ejecute lo siguiente para añadir los registros necesarios:

```
server 127.0.0.1
update add wpad.red-local.net. 86400 A 172.16.1.1
update add red-local.net. 86400 TXT "service: wpad:!http://wpad.red-local.net:80/wpad.dat"
send
quit
```

Utilizando este último procedimiento, es innecesario reiniciar el servicio **named**.

Recuerde que este método jamás debe combinarse con el del anuncio del archivo wpad.dat a través de servidor DHCP.

83.2.6.2. Anuncio a través de servidor DHCP.

Se requiere configurar primero el servidor DNS para que incluya un registro que resuelva el nombre wpad.**red-local.net** el cual será utilizado para hacer el anuncio del URI del archivo wpad.dat a través del servidor DHCP.

Asumiendo que tiene configurado y funcionando un servidor DNS con una **zona estática** que resuelve los nombres de anfitrión y direcciones IP de la red de área local, edite el archivo de zona correspondiente:

```
vim /var/named/data/red-local.net.zone
```

Cambie el número de serie de la zona y añada sólo el siguiente registro en la zona de reenvío en el DNS utilizado por la red de área local. En el ejemplo se asume que el servidor HTTP que hospeda al archivo wpad.dat corresponde a la dirección IP **172.16.1.1**:

```
wpad    IN      A       172.16.1.1
```

Reinicie el servicio **named**.

```
service named restart
```

Si se trata de una **zona dinámica**, utilice el mandato **nsupdate** para conectarse al servidor DNS:

```
nsupdate -k /etc/rndc.key
```

Desde el intérprete de mandatos de **nsupdate**, ejecute lo siguiente para añadir el registro necesario:

```
server 127.0.0.1
update add wpad.red-local.net. 86400 A 172.16.1.1
send
quit
```

Utilizando este procedimiento, es innecesario reiniciar el servicio **named**.

Asumiendo que tiene configurado y funcionando un servidor DHCP para gestionar la asignación de las direcciones IP utilizadas por la red de área local, edite el archivo **/etc/dhcp/dhcpd.conf**:

```
vim /etc/dhcp/dhcpd.conf
```

Añada en la configuración del servidor DHCP, las dos siguientes opciones:

```
option wpad-url code 252 = text;
option wpad-url "http://wpad.red-local.net/wpad.dat\n";
```

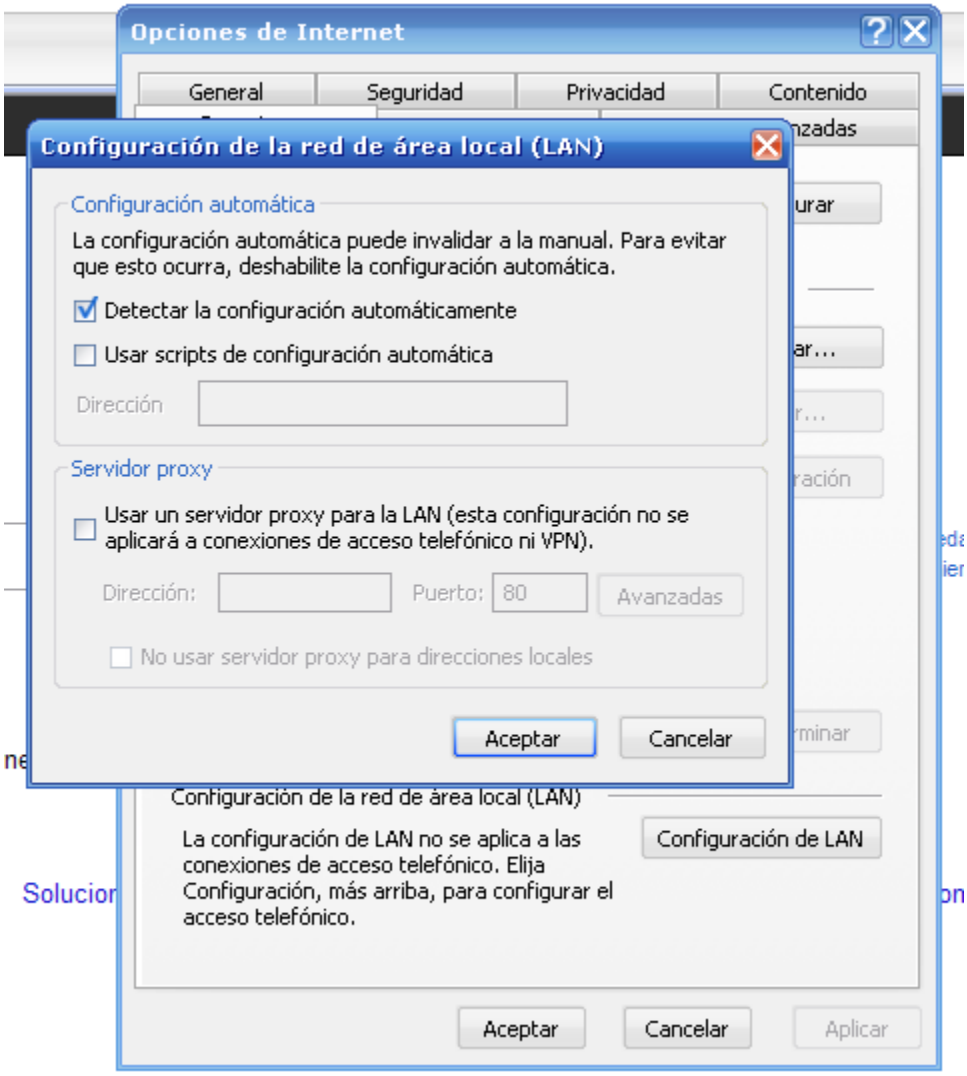
Reinicie el servicio **dhcpd**.

```
service dhcpd restart
```

Recuerde que este método jamás debe combinarse con el del anuncio del archivo wpad.dat a través de servidor DNS.

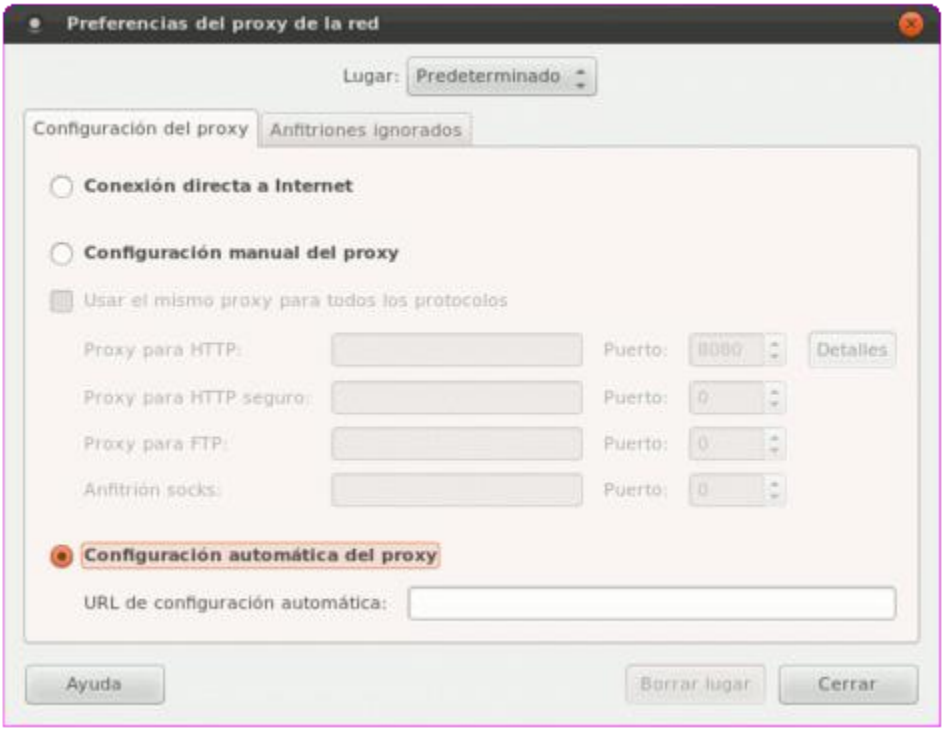
83.2.7. Comprobaciones.

Si todo lo anterior concluyó sin errores, sólo resta verificar que la configuración de los anfitriones con Windows. Vaya a *Opciones de Internet* → *Conexiones* → *Configuración LAN* y verifique que esté habilitada la casilla *Autodetectar configuración de proxy*. En algunos casos es posible que se tenga que definir también el URI del archivo de configuración (*http://wpad.**red-local.net**/wpad.dat*).



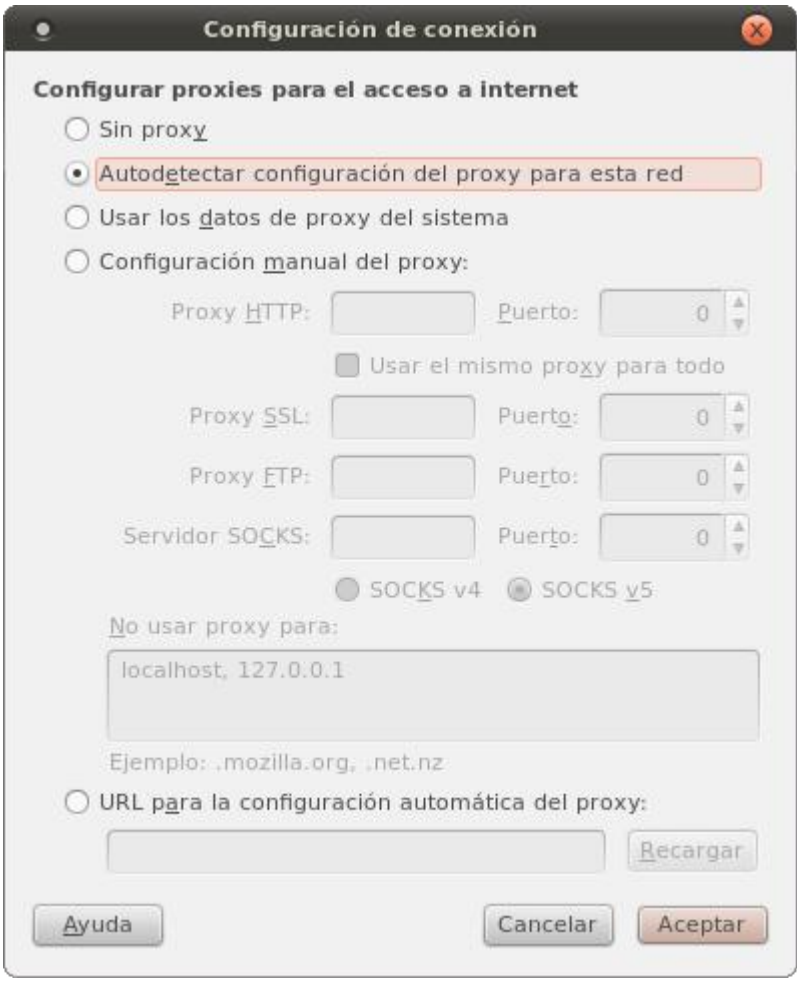
Opciones de Internet - Configuración de Proxy.

Para los anfitriones con GNU/Linux con GNOME 2 como escritorio sólo hay que establecer *Configuración automática del Proxy* en las *Preferencias de Proxy de la red*. Deje vacío el campo de *URL de configuración automática* para forzar la detección del archivo wpad.dat anunciado.



Configuración de Proxy de la red en GNOME 2.

También pude configurar las opciones de cada navegador que lo requiera para que auto-detecte la configuración del servidor proxy.



Opciones de Firefox - autodetectar configuración del proxy.

84. Instalación y configuración de la herramienta de reportes Sarg.

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

84.1. Introducción.

Sarg (**S**quid **A**nalysis **R**eport Generator) es la más completa y fácil de utlizar herramienta para la generación de reportes a partir de las bitácoras de **Squid**. Permite ver con detalle la activida de todos los equipos y/o usuarios dentro de la red de áreal local, registrada en la bitácora de Squid.

URL: http://sarg.sourceforge.net/.

84.2. Equipamiento lógico necesario.

Este documento fue diseñado para ser puesto en práctica exclusivamente en **CentOS 5**, **Elastix 1.5**, **Red Hat Enterprise Linux 5** y **Whitebox Enterprise Linux 5** o sistemas operativos similares, basados sobre **Red Hat Enterprise Linux 5**.

Ingrese al sistema como el usuario **root**.

Proceda a configurar el depósito YUM de Alcance Libre:

```
cd /etc/yum.repos.d/
wget -N http://www.alcancelibre.org/al/server/AL-Server.repo
cd -
```

Instale los paquetes **sarg** y **httpd**, ejecutando lo siguiente:

```
yum -y install sarg httpd
```

84.3. Procedimientos.

Configure el soporte al español para Sarg.

Edite con vim el archivo **/etc/sarg/sarg.conf**:

```
vim /etc/sarg/sarg.conf
```

Alrededor de la línea 30, localice la cadena de texto **language English**.

Pulse la tecla **Insert**.

```
#               Russian_koi8
#               Russian_UFT-8
#               Russian_windows1251
#               Serbian
#               Slovak
#               Spanish
#               Turkish
#
language English

# TAG:  access_log file
#       Where is the access.log file
#       sarg -l file
#
#access_log /usr/local/squid/var/logs/access.log
access_log /var/log/squid/access.log
```

Reemplace la cadena de texto con **language Spanish**.

```
#               Russian_koi8
#               Russian_UFT-8
#               Russian_windows1251
#               Serbian
#               Slovak
#               Spanish
#               Turkish
#
language Spanish

# TAG:  access_log file
#       Where is the access.log file
#       sarg -l file
#
#access_log /usr/local/squid/var/logs/access.log
access_log /var/log/squid/access.log
```

Alrededor de la línea 213, localice la cadena **lastlog 0**.

```
# TAG: lastlog n
#      How many reports files must be keept in reports directory.
#      The oldest report file will be automatically removed.
#      0 - no limit.
#
# lastlog 0
```

Descomente la línea **lastlog 0** y cambie el cero por el número de reportes que se desea mantener. Si define el valor **30**, sólo se conservarán los 30 últimos reportes y todos los reportes anteriores se irán eliminando automáticamente.

```
# TAG: lastlog n
#      How many reports files must be keept in reports directory.
#      The oldest report file will be automatically removed.
#      0 - no limit.
#
lastlog 30
```

Si se omite definir un valor adecuado para la opción **lastlog**, los reportes de almacenarán en **/var/www/sarg/** y pueden implicar una cantidad considerable de datos. Si decide omitir un valor para esta opción, periódicamente tendrá que ingresar a los subdirectorios de **/var/www/sarg/**, principalmente el subdirectorio **daily**, para eliminar de manera manual los reportes antiguos o que sean de poca utilidad, a fin de evitar se agote el espacio en disco duro.

Pulse la tecla **Esc**, guarde cambios y salga de vim pulsando la combinación de teclas **:x** y luego la tecla ⏎ (**ENTER**).

Edite con vim el archivo **/etc/httpd/conf.d/sarg.conf**:

```
vim /etc/httpd/conf.d/sarg.conf
```

Pulse la tecla **Insert**.

Localice la línea **allow from 127.0.0.1**, la cual define que solo se puede acceder hacia el directorio **/sarg/** desde **127.0.0.1** (es decir, solo puede ser accedido como *http://127.0.0.1/sarg/*).

```
Alias /sarg /var/www/sarg
<Directory /var/www/sarg>
        DirectoryIndex index.html
        order deny,allow
        deny from all
        allow from 127.0.0.1
</Directory>
```

Asumiendo que su red de área local corresponde a **172.16.123.0/28**, defina que también se puede acceder al directorio **/sarg/** desde **172.16.123.0/28**, reemplazando por **allow from 127.0.0.1** por **allow from 127.0.0.1 172.16.123.0/28**.

```
Alias /sarg /var/www/sarg
<Directory /var/www/sarg>
        DirectoryIndex index.html
        order deny,allow
        deny from all
        allow from 127.0.0.1 172.16.123.0/28
</Directory>
```

Defina que el acceso hacia el directorio **/sarg/** (que en adelante podrá ser accedido como *http://**proxy.red-local.net**/sarg/* o bien *http://**172.16.123.123**/sarg/*) se permitirá solo a usuarios autorizados que autenticarán a través del archivo **/var/www/claves-sarg**.

```
Alias /sarg /var/www/sarg
<Directory /var/www/sarg>
        DirectoryIndex index.html
        order deny,allow
        deny from all
        allow from 127.0.0.1 172.16.123.0/28
        AuthName "Solo usuarios autorizados."
        AuthType Basic
        require valid-user
        AuthUserFile /var/www/claves-sarg
</Directory>
```

Pulse la tecla **Esc**, guarde cambios y salga de vim pulsando la combinación de teclas **:x** y luego la tecla ⏎ (**ENTER**).

Genere con el mandato **touch** el archivo **/var/www/claves-sarg**:

```
touch /var/www/claves-sarg
```

Utilice el mandato **chmod** para definir que el archivo **/var/www/claves-sarg** solo tendrá permisos de lectura y escritura para la clase del usuario:

```
chmod 0600 /var/www/claves-sarg
```

Utilice el mandato **chown** para definir que el archivo **/var/www/claves-sarg** pertenece al usuario apache y grupo apache:

```
chown apache:apache /var/www/claves-sarg
```

Utilice el mandato **htpasswd** sobre el archivo **/var/www/claves-sarg** para crear el usuario virtual **administrador** y asignar a éste una clave de acceso que solo deberá conocer el administrador del servidor:

```
htpasswd /var/www/claves-sarg administrador
```

Inicie o reinicie si es el caso, el servicio **httpd**.

```
service httpd start
```

Si el servicio **httpd** inició (o reinició) sin errores, utilice el mandato **chkconfig** para que el servicio **httpd** inicie automáticamente junto con el sistema operativo.

```
chkconfig httpd on
```

Con la finalidad de generar datos en las bitácoras del servicio **squid**, permita a la red de área local opere normalmente durante algunos minutos y luego ejecute el mandato **sarg** para generar un primer reporte manual.

```
sarg
```

Podrá consultar este reporte en la dirección *http://**proxy**.**red-local.net**/sarg/ONE-SHOT/* o bien *http://**172.16.123.123**/sarg/ONE-SHOT/*.

Podrá ver un reporte generado automáticamente todos los días en la dirección *http://**proxy**.**red-local.net**/sarg/daily/* o bien *http://**172.16.123.123**/sarg/daily/*.

85. Configuración de OpenVPN.

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

85.1. Introducción.

85.1.1. Acerca de OpenVPN.

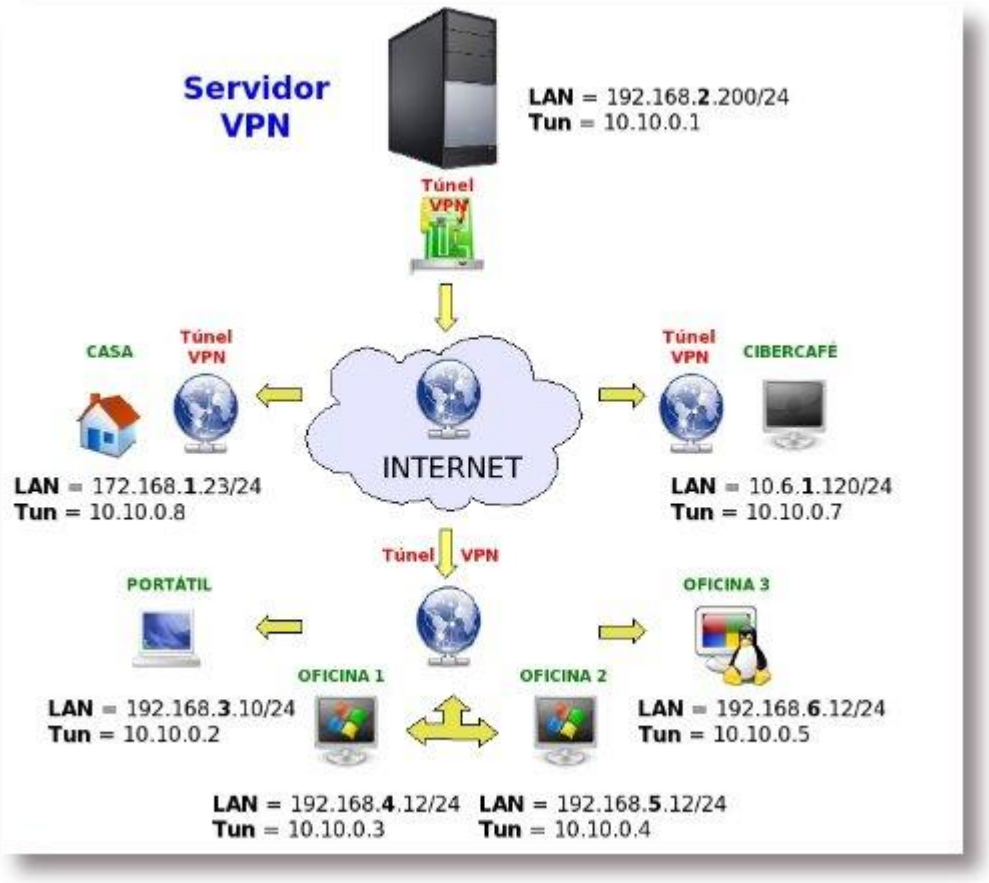
OpenVPN es una solución de conectividad basada sobre equipamiento lógico (*software*): SSL(Secure Sockets Layer) VPN (Virtual Private Network o red virtual privada), OpenVPN ofrece conectividad punto-a-punto con validación, jerárquica de usuarios y host conectados remotamente, resulta una muy buena opción en tecnologías Wi-Fi (redes inalámbricas EEI 802.11) y soporta un amplio tipo configuraciones.

URL: http://openvpn.net

85.1.2. Breve explicación de lo que se logrará con este documento.

Este documento describe la configuración de una **VPN** tipo **Intranet**.

Este tipo de redes es creado entre una oficina central (servidor) y una o varias oficinas remotas (clientes). El acceso viene del exterior. Se utiliza este tipo de VPN cuando se necesita enlazar a los sitios que son parte de una compañía, en este caso se compone de un servidor central para muchos clientes VPN.



Servidor de Pasarela OpenVPN con clientes (Windows/Linux) remotos

El servidor VPN **hace de pasarela** para que todos los clientes OpenVPN.

85.2. Instalación del equipamiento lógico necesario.

85.2.1. Instalación en CentOS.

Como el usuario **root**, desde una terminal, descargue el archivo **AL-Server.repo**:

```
wget -O /etc/yum.repos.d/AL-Server.repo \
    http://www.alcancelibre.org/al/server/AL-Server.repo
```

Instalar los paquetes necesarios:

```
yum -y install openvpn shorewall
```

85.3. Procedimientos.

Si fuera necesario, cambiarse al usuario **root** utilizando el siguiente mandato:

```
su -l
```

Cambie al directorio **/etc/openvpn**:

```
cd /etc/openvpn/
```

NOTA: Todos los procedimientos necesarios para configurar un servidor con **OpenVPN** se realizan sin salir de **/etc/openvpn/**. Por favor, **evite cambiar de directorio** hasta haber finalizado los procedimientos descritos en este documento.

A fin de facilitar los procedimientos, se copiarán los archivos **openssl-1.0.0.cnf**, **whichopensslcnf**, **pkitool** y **vars** —que se localizan dentro del directorio **/usr/share/easy-rsa/**— dentro del directorio **/etc/openvpn/**:

```
cp /usr/share/easy-rsa/openssl-1.0.0.cnf ./
cp /usr/share/easy-rsa/whichopensslcnf ./
cp /usr/share/easy-rsa/pkitool ./
cp /usr/share/easy-rsa/vars ./
```

Utilizar el editor de texto y abrir el archivo **/etc/openvpn/vars**:

```
vi /etc/openvpn/vars
```

De este archivo sólo hay que editar las últimas líneas, que corresponden a algo similar a lo siguiente:

```
export KEY_SIZE=1024
export KEY_COUNTRY="US"
export KEY_PROVINCE="CA"
export KEY_CITY="SanFrancisco"
export KEY_ORG="Fort-Funston"
export KEY_EMAIL="me@myhost.mydomain"
export KEY_EMAIL=mail@host.domain
export KEY_CN=changeme
export KEY_NAME=chanegme
export KEY_OU=changeme
```

Hay que establecer el certificado a 2048 bits para mayor seguridad, reemplazar los valores predeterminados por los que se consideren pertinentes —sin utilizar acentos o tildes— y eliminar la línea repetida que define el correo electrónico predeterminado. Ejemplo:

```
export KEY_SIZE=2048
export KEY_COUNTRY="MX"
export KEY_PROVINCE="DF"
export KEY_CITY="Mexico"
export KEY_ORG="Mi Empresa, S.A. de C.V."
export KEY_EMAIL="fulanito@mi-dominio.com"
export KEY_CN=servidor.mi-dominio.com
export KEY_NAME=servidor
export KEY_OU=Sistemas
```

Se requiere ejecutar del siguiente modo el archivo **/etc/openvpn/vars** a fin de que carguen las variables de entorno que se acaban de configurar.

```
source /etc/openvpn/./vars
```

Cada vez que se vayan a generar nuevos certificados, debe ejecutarse el mandato anterior a fin de que carguen las variables de entorno definidas.

Se ejecuta el archivo **/usr/share/easy-rsa/clean-all** a fin de limpiar cualquier firma digital que accidentalmente estuviera presente.

```
sh /usr/share/easy-rsa/clean-all
```

Lo anterior realiza un **rm -fr** (eliminación recursiva) sobre el directorio **/etc/openvpn/keys**, por lo que se eliminarán todas los certificados y firmas digitales que hubieran existido con anterioridad.

A fin de crear el certificado del servidor, se crea un certificado:

```
sh /usr/share/easy-rsa/build-ca
```

Se creará el archivo dh2048.pem, el cual contendrá las opciones del protocolo **D**iffie-**H**ellman, de 2048 bits:

```
sh /usr/share/easy-rsa/build-dh
```

El protocolo **D**iffie-**H**ellman permite el intercambio secreto de claves entre dos partes que sin que éstas hayan tenido contacto previo, utilizando un canal inseguro y de manera anónima (sin autenticar). Se emplea generalmente como medio para acordar claves simétricas que serán empleadas para el cifrado de una sesión, como es el caso de una conexión VPN.

Para generar la firma digital, se utilizan el siguiente mandato:

```
sh /usr/share/easy-rsa/build-key-server server
```

Finalmente se crean los certificados para los clientes. En el siguiente3 ejemplo se crean los certificados para **cliente1**, **cliente2**, **cliente3**, **cliente4**, **cliente5** y **cliente6**:

```
sh /usr/share/easy-rsa/build-key cliente1
sh /usr/share/easy-rsa/build-key cliente2
sh /usr/share/easy-rsa/build-key cliente3
sh /usr/share/easy-rsa/build-key cliente4
sh /usr/share/easy-rsa/build-key cliente5
sh /usr/share/easy-rsa/build-key cliente6
```

A fin de utilizar los certificados y que se configure el sistema, se crea con el editor de texto el archivo **/etc/openvpn/servidorvpn-udp-1194.conf**, donde *servidorvpn* se reemplaza por el nombre de anfitrión del sistema:

```
vi /etc/openvpn/servidorvpn-udp-1194.conf
```

Para la **VPN** se recomienda utilizar una red privada que sea poco usual, a fin de poder permitir a los clientes conectarse sin conflictos de red. Un ejemplo de una red poco utilizada sería 192.168.37.0/255.255.255.0, lo cual permitirá conectarse a la **VPN** a 253 clientes. Tomando en cuenta lo anterior, el contenido del archivo **/etc/openvpn/servidorvpn-udp-1194.conf**, debe ser el siguiente:

```
port 1194
proto udp
dev tun
#----- Sección de firma y certificados -----
ca keys/ca.crt
cert keys/server.crt
key keys/server.key
dh keys/dh2048.pem
#-----------------------------------------
server 192.168.37.0 255.255.255.0
ifconfig-pool-persist ipp.txt
keepalive 10 120
comp-lzo
persist-key
persist-tun
status openvpn-status-servidorvpn-udp-1194.log
verb 3
```

Descripción de las opciones anteriores:

Port: Especifica el puerto que será utilizado para que los clientes vpn puedan conectarse al servidor.

Proto: tipo de protocolo que se empleará en a conexión a través de VPN

dev: Tipo de interfaz de conexión virtual que se utilizará el servidor openvpn.

ca: Especifica la ubicación exacta del archivo de Autoridad Certificadora [.ca].

cert: Especifica la ubicación del archivo [.crt] creado para el servidor.

key: Especifica la ubicación de la llave [.key] creada para el servidor openvpn.

dh: Ruta exacta del archivo [.pem] el cual contiene el formato de Diffie Hellman (requirerido para **--tls-server**solamente).

server: Se asigna el rango IP virtual que se utilizará en la red del túnel VPN.

Ifconfig-pool-persist: Archivo en donde quedarán registrado las direcciones IP de los clientes que se encuentran conectados al servidor OpenVPN.

Keepalive 10 120 : Envía los paquetes que se manejan por la red una vez cada 10 segundos; y asuma que el acoplamiento es abajo si ninguna respuesta ocurre por 120 segundos.

comp-lzo: Especifica los datos que recorren el túnel vpn será compactados durante la trasferencia de estos paquetes.

persist-key: Esta opción soluciona el problema por llaves que persisten a través de los reajustes SIGUSR1, así que no necesitan ser releídos.

Persist-tun: Permite que no se cierre y re-abre los dispositivos TAP/TUN al correr los guiones up/down

status: archivo donde se almacenará los eventos y datos sobre la conexión del servidor [.log]

verb: Nivel de información (default=1). Cada nivel demuestra todo el Info de los niveles anteriores. Se recomienda el nivel 3 si usted desea un buen resumen de qué está sucediendo.

0 --No muestra una salida excepto errores fatales. **1 to 4 –**Rango de uso normal. **5 --**Salida **R**y **W**caracteres en la consola par los paquetes de lectura y escritura, mayúsculas es usada por paquetes TCP/UDP minúsculas es usada para paquetes TUN/TAP.

Si **SELinux** está activo, es necesario que el directorio **/etc/openvpn** y sus contenidos, tengan los contextos apropiados de esta implementación de seguridad (system_u:object_r:**openvpn_etc_rw_t** para **ipp.txt** y **openvpn-status-servidorvpn-udp-1194.log** y system_u:object_r:**openvpn_etc_t** para el resto del contenido del directorio).

Se utiliza luego el mandato **restorecon** sobre el directorio **/etc/openvpn** a fin de asignar los contextos adecuados.

```
restorecon -R /etc/openvpn/
```

Asumiendo que aún se encuentra dentro del directorio **/etc/openvpn**, genere los archivos **ipp.txt** y **openvpn-status-servidorvpn-udp-1194.log** utilizando el mandato **touch**:

```
touch ipp.txt
touch openvpn-status-servidorvpn-udp-1194.log
```

Si se tiene activo SELinux, estos últimos dos archivos requieren se les asigne contexto de lectura y escritura (**openvpn_etc_rw_t**).

```
chcon -u system_u *.txt *.log
chcon -r object_r *.txt *.log
chcon -t openvpn_etc_rw_t *.txt *.log
```

Los anterior cambia los contextos a usuario de sistema (**system_u**), rol de objeto (**object_r**) y tipo configuración de OpenVPN de lectura y escritura (**openvpn_etc_rw_t**).

Para iniciar el servicio, se utiliza el mandato **service** del siguiente modo:

```
service openvpn start
```

Para que el servicio de OpenVPN esté activo en el siguiente inicio del sistema, se utiliza el mandato **chkconfig** de la siguiente forma:

```
chkconfig openvpn on
```

85.3.1. Configuración de muro cortafuegos con Shorewall.

El siguiente procedimiento considera que se ha configurado un muro cortafuegos apropiadamente, de acuerdo a las indicaciones descritas en el documento titulado **Cómo configurar un muro cortafuegos con Shorewall y tres interfaces de red**.

Edite el archivo **/etc/shorewall/zones**:

```
vi /etc/shorewall/zones
```

Independientemente del contenido, añada la zona **rem** con el tipo **ipv4**.

```
rem     ipv4
```

Edite el archivo **/etc/shorewall/interfaces**:

```
vi /etc/shorewall/interfaces
```

Independientemente del contenido, añada la zona **rem** asociada a la interfaz **tun0**, con la opción **detect**, para detectar automáticamente el número de dirección **IP** de difusión (*broadcast*) y la opción **dhcp**.

```
rem     tun0            detect          dhcp
```

Edite el archivo **/etc/shorewall/policy**:

```
vi /etc/shorewall/policy
```

Independientemente del contenido, añada las políticas deseadas para permitir el acceso de los miembros de la **VPN** hacia las zonas que se consideren apropiadas. En el siguiente ejemplo, se definen una sola política que permite el acceso desde la zona **rem** hacia cualquier otra zona del muro cortafuegos.

```
rem             all             ACCEPT
```

Si así lo requiere, puede definir políticas individuales hacia cada zona. En el siguiente ejemplo, se definen tres políticas que permiten el acceso desde la zona **rem** hacia la zonas fw, loc y net del muro cortafuegos.

```
rem             fw              ACCEPT
rem             net             ACCEPT
rem             loc             ACCEPT
```

Edite el archivo **/etc/shorewall/rules**:

```
vi /etc/shorewall/rules
```

Independientemente del contenido, añada una regla para abrir el puerto 1194 por UDP para todas las conexiones iniciadas desde la zona net:

```
ACCEPT  net     fw      udp     1194
```

Nota.

Sólo si se desea transparentar el tráfico entre la VPN y la red de área local, añada las reglas para permitir enmascarar el tráfico proveniente de la interfaz del túnel de la VPN hacia la interfaz de la zona de la red de área local y viceversa.

Edite el archivo **/etc/shorewall/masq**:

```
vi /etc/shorewall/masq
```

Añada lo siguiente:

```
eth1    tun0
tun0    eth1
```

Edite el archivo **/etc/shorewall/tunnels**:

```
vi /etc/shorewall/tunnels
```

Defina la configuración de tunel tipo servidor OpenVPN operando por puerto 1194, utilizando la zona **rem** y permitiendo conectarse desde cualquier ubicación.

```
#TYPE                   ZONE    GATEWAY         GATEWAY
#                                               ZONE
openvpnserver:1194      rem     0.0.0.0/0
```

En lugar de **0.0.0.0/0** también puede especificar una dirección IP o bien un segmento de red desde la cual se quiera establecer las conexiones **VPN**.

Para aplicar los cambios, es necesario reiniciar **shorewall** con el mandato **service**, del siguiente modo:

```
service shorewall restart
```

85.3.2. Configuración de clientes Windows.

85.3.2.1. A través de OpenVPN GUI.

Instalar el paquete de **OpenVPN** para Windows desde http://openvpn.net/index.php/open-source/downloads.html.

Crear el archivo **cliente1-udp-1194.ovpn**, con el siguiente contenido, donde es importante que las rutas definidas sean las correctas y las diagonales invertidas sean dobles:

```
client
dev tun
proto udp
remote dominio-o-ip.del.servidor.vpn 1194
float
resolv-retry infinite
nobind
persist-key
persist-tun
#------ SECCION DE LLAVES --------
ca "C:\\Archivos de Programa\\OpenVPN\\config\\ca.crt"
cert "C:\\Archivos de Programa\\OpenVPN\\config\\cliente1.crt"
key "C:\\Archivos de Programa\\OpenVPN\\config\\cliente1.key"
ns-cert-type server
#--------------------------------
comp-lzo
verb 3
```

Descripción de las opciones anteriores:

client: Especifica el tipo de configuración, en este caso tipo cliente OpenVPN.

Port: Especifica el puerto que será utilizado para que los clientes VPN puedan conectarse al servidor.

Proto: tipo de protocolo que se empleará en a conexión a través de VPN

dev: Tipo de interfaz de conexión virtual que se utilizará el servidor openvpn.

remote: Host remoto o dirección IP en el cliente, el cual especifica al servidor OpenVPN.

El cliente OpenVPN puede tratar de conectar al servidor con **host:port** en el orden especificado de las opciones de la opción **--remote**.

float: Este le dice a OpenVPN aceptar los paquetes autenticados de cualquier dirección, no solamente la dirección cuál fue especificado en la opción **--remote**.

resolv-retry: Si la resolución del nombre del anfitrión (*hostname*) falla para **-- remote**, la resolución antes de fallar hace una re-comprobación de n segundos.

nobind: No agrega bind a la dirección local y al puerto.

ca: Especifica la ubicación exacta del archivo de Autoridad Certificadora [.ca].

cert: Especifica la ubicación del archivo [.crt] creado para el servidor.

key: Especifica la ubicación de la llave [.key] creada para el servidor OpenVPN.

remote: Especifica el dominio o IP del servidor así como el puerto que escuchara las peticiones para servicio VPN.

comp-lzo: Especifica los datos que recorren el túnel VPN será compactados durante la trasferencia de estos paquetes.

persist-key: Esta opción soluciona el problema por llaves que persisten a través de los reajustes SIGUSR1, así que no necesitan ser releídos.

Persist-tun: Permite que no se cierre y re-abre los dispositivos TAP/TUN al correr los guiones up/down

verb: Nivel de información (default=1). Cada nivel demuestra toda la Información de los niveles anteriores. Se recomienda el nivel 3 si usted desea un buen resumen de qué está sucediendo.

0 --No muestra una salida excepto errores fatales. **1 to 4 –**Rango de uso normal. **5 --**Salida **R**y **W**caracteres en la consola par los paquetes de lectura y escritura, mayúsculas es usada por paquetes TCP/UDP minúsculas es usada para paquetes TUN/TAP.

El cliente necesitará que los archivos **ca.crt**, **cliente1.crt**, **cliente1.key** y **cliente1-udp-1194.ovpn** estén presentes en el directorio **"C:\Archivos de Programa\OpenVPN\config\"**. Estos archivos fueron creados, a través de un procedimiento descrito en este documento, dentro del directorio **/etc/openvpn/keys/** del servidor.

Si se quiere que los clientes de la **VPN** se puedan conectar a la red local, es importante considerar las implicaciones de seguridad que esto conlleva si alguno de los certificados es robado o bien el cliente se ve comprometido en su seguridad por una intrusión, virus, troyano o gusano. Es preferible que la red de la **VPN** sea independiente a la red local y cualquier otra red, uniendo los servidores y clientes a la **VPN**, independientemente de si éstos están en la red local o una red pública.

Si es imperativo hacer que los clientes de la **VPN** se conecten a la red local, la red desde la cual se conectan los clientes debe ser diferente a la red utilizada en la red local. Por ejemplo: si la red local detrás del servidor de **VPN** es 192.168.0.0/255.255.255.0, 10.0.0.0/255.0.0.0 o 172.16.0.0/255.255.0.0, los clientes que se conecten a la **VPN** detrás de un modem ADSL o Cable e intenten establecer conexiones con la red local, muy seguramente tendrán conflictos de red.

Para permitir a los clientes de la **VPN** poder establecer conexiones hacia la red local, se añaden las siguientes líneas en el archivo de configuración de OpenVPN para los clientes y que definen la ruta para la red local y un servidor DNS que debe estar presente y configurado para permitir **consultas recursivas** a la red de la **VPN**:

```
route 192.168.0.0 255.255.255.0
dhcp-option DNS 192.168.0.1
```

Opcionalmente, también se puede definir un servidor Wins.

```
dhcp-option WINS 192.168.26.1
```

Ejemplo, donde se asume que la red de área local corresponde a 192.168.26.0/255.255.255.0 y el servidor DNS y WINS corresponde a 192.168.26.1:

```
client
dev tun
proto udp
remote dominio-o-ip.del.servidor.vpn 1194
float
resolv-retry infinite
nobind
persist-key
persist-tun
route 192.168.26.0 255.255.255.0
dhcp-option DNS 192.168.26.1
dhcp-option WINS 192.168.26.1
#------ SECCION DE LLAVES --------
ca "C:\\Archivos de Programa\\OpenVPN\\config\\ca.crt"
cert "C:\\Archivos de Programa\\OpenVPN\\config\\cliente1.crt"
key "C:\\Archivos de Programa\\OpenVPN\\config\\cliente1.key"
ns-cert-type server
#---------------------------------
comp-lzo
verb 3
```

85.3.3. Clientes GNU/Linux.

85.3.3.1. A través del servicio openvpn.

Este es el método que funcionará en prácticamente todas las distribuciones de de GNU/Linux basadas sobre **Red Hat**, **CentOS** y **Fedora**. Se requiere instalar el paquete **openvpn**:

```
yum -y install openvpn
```

Para **CentOS** y **Red Hat™ Enterprise Linux**, se requiere haber configurado previamente el almacén YUM de **AL Server**, descrito con anterioridad en este mismo documento.

Para los clientes con GNU/Linux utilizando el servicio **openvpn**, básicamente se utiliza el mismo archivo para **OpenVPN GUI** para Windows, pero definiendo rutas en el sistema de archivos de GNU/Linux. Ejemplo:

```
client
dev tun
proto udp
remote dominio-o-ip.del.servidor.vpn 1194
float
resolv-retry infinite
nobind
persist-key
persist-tun
#------ SECCION DE LLAVES --------
ca /etc/openvpn/keys/ca.crt
cert /etc/openvpn/keys/cliente1.crt
key /etc/openvpn/keys/cliente1.key
ns-cert-type server
#---------------------------------
comp-lzo
verb 3
```

Si se desea enrutar hacia la red de área local detrás del servidor, se utiliza una configuración similar a la de los clientes con Windows, añadiendo las opciones resaltadas en negrita, donde se asume que la red de área local corresponde a 192.168.26.0/255.255.255.0 y el servidor DNS corresponde a 192.168.26.1:

```
client
dev tun
proto udp
remote dominio-o-ip.del.servidor.vpn 1194
float
resolv-retry infinite
nobind
persist-key
persist-tun
route 192.168.26.0 255.255.255.0
dhcp-option DNS 192.168.26.1
#------ SECCION DE LLAVES --------
ca /etc/openvpn/keys/ca.crt
cert /etc/openvpn/keys/cliente1.crt
key /etc/openvpn/keys/cliente1.key
ns-cert-type server
#-------------------------------
comp-lzo
verb 3
```

Este archivo se guarda como **/etc/openvpn/cliente1-udp-1194.ovpn**. Requiere que los certificados definidos en la configuración estén en las rutas especificadas dentro del directorio **/etc/openvpn/keys/**.

Para iniciar la conexión hacia la **VPN**, simplemente se inicia el servicio **openvpn**:

```
service openvpn start
```

Para que la conexión se establezca automáticamente cada vez que se inicie el sistema, se utiliza el mandado **chkconfig** de la siguiente manera:

```
chkconfig openvpn on
```

85.3.3.2. A través de NetworkManager.

NetworkManager es una implementación que permite a los usuarios configurar interfaces de red de todos los tipos, sin necesidad de contar con privilegios de administración en el sistema. Es la forma más flexible, sencilla y práctica de conectarse a una red **VPN**.

Se requiere que los clientes Linux tengan instalado el paquete **NetworkManager-openvpn**, mismo que debe estar incluido en lo almacenes YUM de **Fedora** y distribuciones recientes de GNU/Linux. **CentOS** y **Red Hat™ Enterprise Linux** carecen los paquetes necesarios para utilizar **NetworkManager-openvpn**, por lo que solo podrá conectarse a la **VPN** a través del método anterior, con el servicio **openvpn**.

Para instalar a través del mandato **yum** en distribuciones basadas sobre **Fedora 9** en adelante, se hace de la siguiente manera:

```
yum -y install NetworkManager-openvpn
```

Se puede reiniciar el sistema para que tengan efectos los cambios o simplemente reiniciar el servicio **NetworkManager**:

```
service NetworkManager restart
```

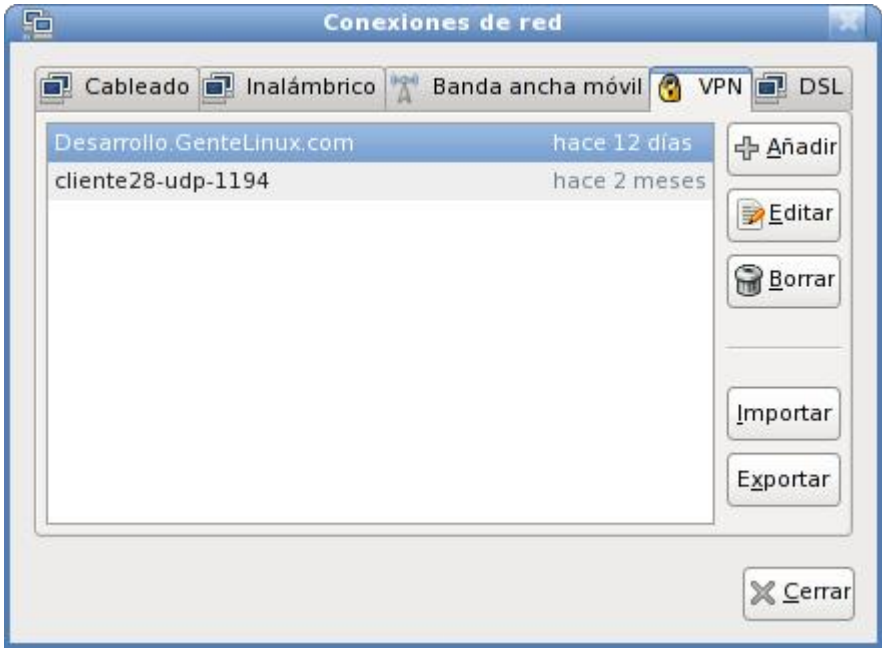
Lo anterior cerrará y volverá a establecer las conexiones de red existentes.

Al igual que el método anterior, para los clientes con GNU/Linux con NetworkManager, básicamente se utiliza el mismo archivo para **OpenVPN GUI** para Windows, pero definiendo rutas en el sistema de archivos de GNU/Linux. Ejemplo:

```
client
dev tun
proto udp
remote dominio-o-ip.del.servidor.vpn 1194
float
resolv-retry infinite
nobind
persist-key
persist-tun
#------ SECCION DE LLAVES --------
ca /etc/openvpn/keys/ca.crt
cert /etc/openvpn/keys/cliente1.crt
key /etc/openvpn/keys/cliente1.key
ns-cert-type server
#--------------------------------
comp-lzo
verb 3
```

Este archivo se puede utilizar con la interfaz gráfica de **NetworkManager**. Solo hay que hacer clic sobre el icono en el **Área de notificación** del panel de GNOME y luego hacer clic en **Configurar VPN**.

En la ventana que abre a continuación, hay un botón que permite importar el archivo de configuración.



Si los certificados y firma digital son colocados en la ruta **/etc/openvpn/keys/** con SELinux activo, éstos funcionarán adecuadamente. Si los certificados y firma digital son almacenados dentro del directorio de inicio del usuarios, es necesario establecer la política **openvpn_enable_homedirs** con valor **1** (que equivale a **on** o activa):

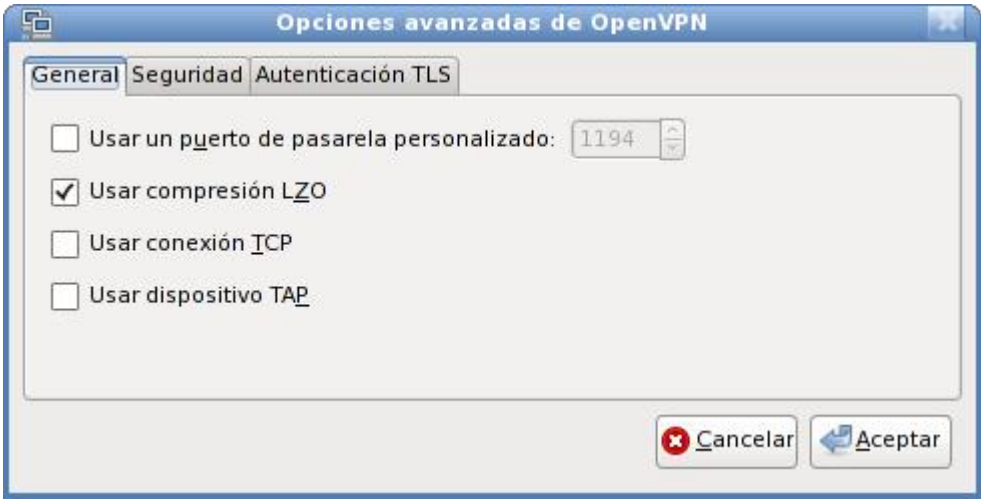
```
setsebool -P openvpn_enable_homedirs 1
```

Personalmente recomiendo crear una configuración nueva desde la interfaz de **NetworkManager**. Desde la ventana de redes VPN de la interfaz de **NetworkManager**, hacer clic en **Añadir**.

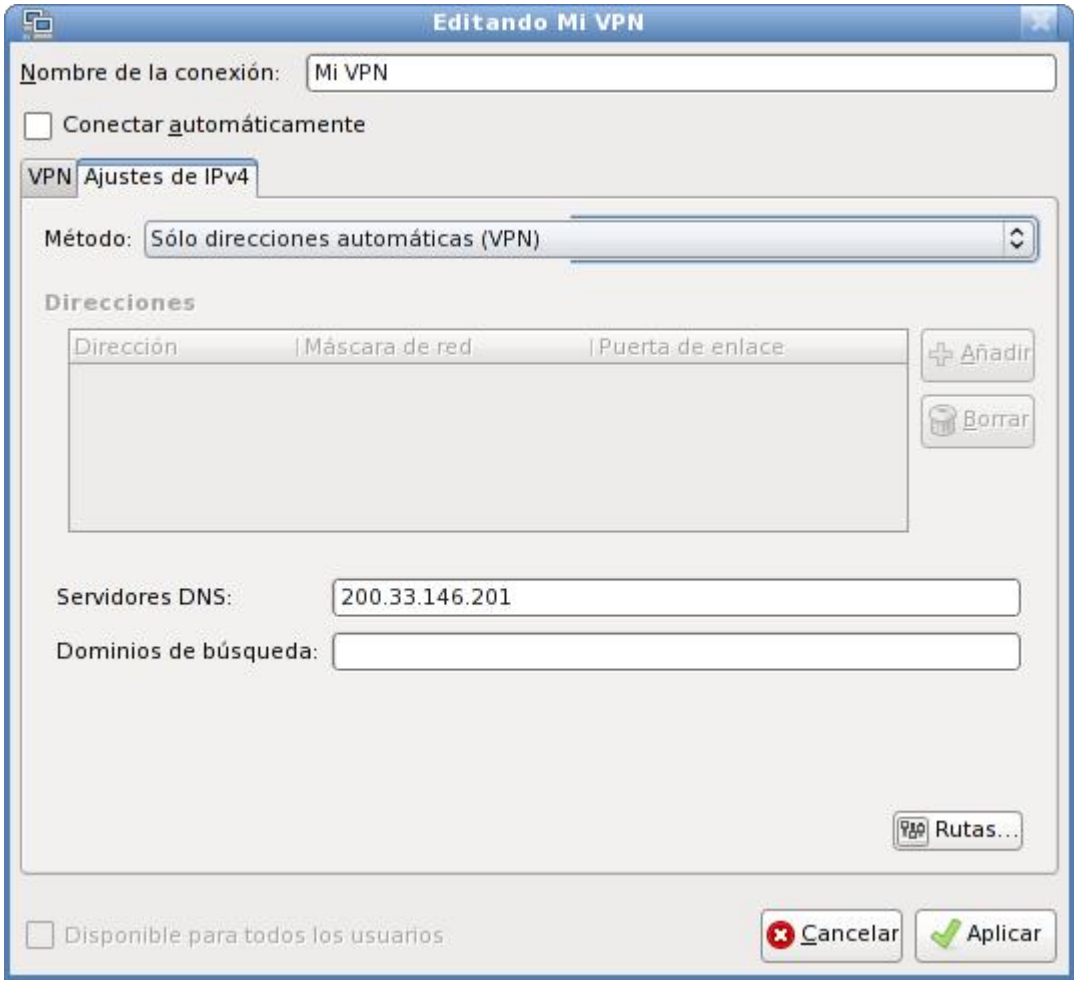
Aparecerá un diálogo donde se debe seleccionar que se trata de una **VPN** con **OpenVPN**.

En la siguiente ventana de diálogo, se define el nombre de la conexión, dirección IP o nombre del servidor donde está instalado OpenVPN y los certificados a utilizar. Si se siguieron los procedimientos de ese documento, se **deja en blanco** el campo **Contraseña de clave privada**.

Luego, se hace clic en **Avanzado** para especificar que se utilizará compresión **LZO**.



Para evitar conflictos de conectividad, se hace clic en la pestaña **Ajustes IPV4** y se define un servidor DNS que permita al cliente navegar a través de Internet y dentro de la red de la **VPN**.



Se hace clic en **Rutas** para abrir otra ventana de diálogo y se seleccionan las casillas de las opciones **Ignorar las rutas obtenidas automáticamente** y **Usar esta conexión solo para los recursos de su red**. Opcionalmente se pueden añadir las rutas estáticas para tener conectividad con la red local detrás del servidor de **VPN**, tomando en cuenta que la red local desde la cual se está conectado el cliente debe ser diferente a la de la red local detrás del servidor de **VPN**, a fin de evitar conflictos de red.

Finalmente se hace clic en aplicar. Para conectarse a la red **VPN**, solo basta hacer clic sobre el icono de **NetworkManager** en el **Área de notificación** del panel de GNOME y seleccionar la red **VPN** recién configurada.

85.4. Bibiliografía.

Este documento se basa sobre los manuales titulados VPN en servidor Linux y clientes Windows/Linux con OpenVPN + Shorewall [Parte 1] y VPN en servidor Linux y clientes Windows/Linux con OpenVPN + Shorewall [Parte 2], por **William López Jiménez**, publicados en **Alcance Libre**, cumpliendo cabalmente con los términos de la licencia **Creative Commons** Reconocimiento-NoComercial-CompartirIgual 2.1.

86. Usando Smartd para anticipar los desastres de disco duro

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. **b) No puede utilizar esta obra para fines comerciales.** c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

86.1. Introducción

La mayoría de las distribuciones recientes incluyen smartctl y smartd (parte de smartmontools incluido en el paquete kernel-utils), que son herramientas utilizadas para supervisar la salud de los discos duros realizando pruebas para comprobar su buen funcionamiento. Mientras el disco y la tarjeta madre (soporte se activa en el BIOS) tengan capacidad para utilizar S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology) es posible anticipar las fallas de un disco duro. Solo basta configurar un archivo (/etc/smartd.conf) e iniciar un servicio (smartd).

86.2. Procedimientos

El archivo `/etc/smartd.conf` solo requiere una línea de configuración por cada disco duro en el sistema. Ejemplos:

```
/dev/hda -a -m alguien@dominio.com
/dev/sda -d scsi -a -m alguien@dominio.com
/dev/sdb -d scsi -a -m alguien@dominio.com
```

Lo anterior hace que se envié un reporte completo y detallado de toda la información S.M.A.R.T. y las alertas pendientes. La opción `-a` en discos IDE equivale a:

```
/dev/hda -H -i -c -A -l error -l selftest -l selective
```

Y en discos SCSI equivale a:

```
/dev/sda -H -i -A -l error -l selftest
```

Donde:

`-H`
Incluye en el reporte el estado de salud y alertas pendientes. Si se quiere enviar reportes a un teléfono móvil, esta sería la opción única a utilizar.

`-i`
Incluye en el reporte el numero de modelo, número de serie, versión de Firmware e información adicional relacionada.

-c
Incluye en el reporte las capacidades S.M.A.R.T.

-A
Incluye en le reporte atributos S.M.A.R.T. específicos del fabricante del disco.

-l error
Incluye en el reporte la bitácora de errores de S.M.A.R.T.

-l selftest
Incluye en el reporte la bitácora de pruebas de S.M.A.R.T.

-l selective
Algunos discos tipo ATA-7 (ejemplo: Maxtor) incluyen una bitácora de pruebas selectivas.

-m
Cuenta de correo electrónico a la cual se enviarán reportes.

Si por ejemplo, solo nos interesa recibir reportes de salud de /**dev/hda**, /**dev/sda** y /**dev/sdb**, en una cuenta de correo electrónico (que puede ser la que coresponda para recibir mensajes en un teléfono móvil), se utilizarían lo siguiente en el archivo /**etc/smartd.conf**:

```
/dev/hda -H -m alguien@dominio.com
/dev/sda -d scsi -H -m alguien@dominio.com
/dev/sdb -d scsi -H -m alguien@dominio.com
```

Hecho lo anterior, solo se necesita agregar el servicio a los servicios de arranque del sistema e iniciar (o reiniciar, según el caso) smartd:

```
chkconfig smartd on
service smartd start
```

El servicio se encarga de ejecutar automáticamente en el tras fondo del sistema todas las pruebas necesarias y soportadas por las unidades de disco duro presentes. El reporte se envía automáticamente junto con el mensaje con el reporte de la bitácora del sistema unos minutos después de las 4:00 AM.

Si se quiere ver un reporte al momento, completo y detallado, suponiendo que se trata de un disco duro en el IDE 1, basta ejecutar:

```
smartctl -a /dev/hda
```

Si se quiere ver un reporte al momento que solo muestre el estado de salud de la unidad, suponiendo que se trata de un disco duro en el IDE 1, basta ejecutar:

```
smartctl -H /dev/hda
```

87. Restricción de acceso a unidades de almacenamiento externo

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. **b) No puede utilizar esta obra para fines comerciales.** c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

87.1. Introducción.

En los entornos corporativos y algunas empresas que utilizan GNU/Linux como sistema operativo de escritorio, es una práctica común bloquear el acceso a unidades de disco óptico y unidades de almacenamiento USB. Hay varias formas de lograr este objetivo. Pueden usarse individualmente o en combinación, dependiendo de lo que prefiera el administrador del sistema.

87.2. Procedimientos.

87.2.1. Bloquear el uso de unidades de disco óptico.

El procedimiento es el mismo para CentOS, Fedora, openSUSE, Red Hat Enterprise Linux y SUSE Linux Enterprise.

Edite el archivo **/etc/fstab**:

```
vim /etc/fstab
```

Añada el siguiente contenido:

```
/dev/dvd    /media/dvd    auto    noauto,defaults    0 0
```

Lo anterior hará que la unidad de disco óptico sólo pueda ser utilizada por root.

Lo anterior se complementa estableciendo como valor obligatorio que jamás se monten automáticamente las unidades de almacenamiento externo.

```
gconftool-2 --direct --config-source \
    xml:readwrite:/etc/gconf/gconf.xml.mandatory \
    /apps/nautilus/preferences/media_automount \
    --type bool false
```

Sólo para SUSE Enterprise Linux 10, la ruta del directorio **gconf.xml.mandatory** corresponde a **/etc/opt/gnome/gconf/gconf.xml.mandatory**:

```
gconftool-2 --direct --config-source \
     xml:readwrite:/etc/opt/gnome/gconf/gconf.xml.mandatory \
    /apps/nautilus/preferences/media_automount \
    --type bool false
```

Concluido lo anterior, si un usuario regular inserta un CD o DVD en la unidad óptica, la unidad jamás será montada y si el usuario intenta montar manualmente le será denegado el acceso mostrando una ventana de alerta.

87.2.2. Bloquear uso del módulo usb-storage o uas del núcleo de Linux.

Es posible bloquear el acceso al módulo **usb-storage** o bien el módulo **uas**, del núcleo de Linux. Éstos son los dos controladores utilizados para acceder a cualquier tipo de unidad de almacenamiento externo por USB.

87.2.3. En CentOS, Fedora y Red Hat Enterprise Linux.

Utilice cualquier editor de texto para **crear** el archivo **/etc/modprobe.d/usb-storage.conf**:

```
vim /etc/modprobe.d/usb-storage.conf
```

Añada el siguiente contenido:

```
install usb-storage /bin/false
```

Reinicie el sistema para que surtan efecto los cambios o bien desconecte cualquier unidad de almacenamiento USB que esté presente en el sistema y ejecute lo siguiente:

```
rmmod usb-storage
depmod -a
```

Inserte cualquier unidad de almacenamiento USB para verificar que es imposible acceder hacia el contenido de ésta.

Si lo prefiere, también es posible permitir cargar el módulo **usb-storage**, pero emitiendo un mensaje de correo electrónico que informará al administrador del sistema cuando se inserte una unidad de almacenamiento USB.

Utilice cualquier editor de texto para crear o modificar el archivo **/etc/modprobe.d/usb-storage.conf**:

Elimine la configuración previa y/o añada el siguiente contenido:

```
install usb-storage /bin/mail \
    -s "Unidad USB insertada en $HOSTANAME" \
    alguien@algo.com
```

Reinicie el sistema para que surtan efecto los cambios o bien desconecte cualquier unidad de almacenamiento USB que esté presente en el sistema y ejecute lo siguiente:

```
rmmod usb-storage
depmod -a
```

Espere unos minutos y verifique el mensaje que ha emitido el sistema en el buzón entrada de la cuenta de correo electrónico definida.

87.2.4. En openSUSE.

En openSUSE se utiliza de modo predeterminado el módulo **uas** (**U**SB **A**ttached **S**CSI), el cual es una alternativa más moderna y que tiene un mejor desempeño y funcionamiento que el módulo **usb-storage**.

Utilice cualquier editor de texto para crear el archivo **/etc/modprobe.d/usb-storage.conf**:

```
vim /etc/modprobe.d/usb-storage.conf
```

Añada el siguiente contenido:

```
install uas /bin/false
```

Reinicie el sistema para que surtan efecto los cambios o bien desconecte cualquier unidad de almacenamiento USB que esté presente en el sistema y ejecute lo siguiente:

```
rmmod uas
depmod -a
```

Inserte cualquier unidad de almacenamiento USB para verificar que es imposible acceder hacia el contenido de ésta.

Si lo prefiere, también es posible permitir cargar el módulo **uas**, pero emitiendo un mensaje de correo electrónico que informará al administrador del sistema cuando se inserte una unidad de almacenamiento USB.

Utilice cualquier editor de texto para crear o modificar el archivo **/etc/modprobe.d/uas.conf**:

Elimine la configuración previa y/o añada el siguiente contenido:

```
install uas /usr/bin/mail \
    -s "Unidad USB insertada en $HOSTANAME" \
    alguien@algo.tld
```

Reinicie el sistema para que surtan efecto los cambios o bien desconecte cualquier unidad de almacenamiento USB que esté presente en el sistema y ejecute lo siguiente:

```
rmmod uas
depmod -a
```

Espere unos minutos y verifique el mensaje que ha emitido el sistema en el buzón entrada de la cuenta de correo electrónico definida.

87.2.5. En SUSE Linux Enterprise.

Utilice cualquier editor de texto para modificar el archivo **/etc/modprobe.conf.local**:

```
vim /etc/modprobe.conf.local
```

Añada el siguiente contenido:

```
install usb-storage /bin/false
```

Reinicie el sistema para que surtan efecto los cambios o bien desconecte cualquier unidad de almacenamiento USB que esté presente en el sistema y ejecute lo siguiente:

```
rmmod usb-storage
depmod -a
```

Inserte cualquier unidad de almacenamiento USB para verificar que es imposible acceder hacia el contenido de ésta.

Si lo prefiere, también es posible permitir cargar el módulo **usb-storage**, pero emitiendo un mensaje de correo electrónico que informará al administrador del sistema cuando se inserte una unidad de almacenamiento USB.

Utilice cualquier editor de texto para modificar el archivo **/etc/modprobe.conf.local**:

```
vim /etc/modprobe.conf.local
```

Elimine la configuración previa y/o añada el siguiente contenido:

```
install usb-storage /usr/bin/mail \
    -s "Unidad USB insertada en $HOSTANAME" \
    alguien@algo.com
```

Reinicie el sistema para que surtan efecto los cambios o bien desconecte cualquier unidad de almacenamiento USB que esté presente en el sistema y ejecute lo siguiente:

```
rmmod usb-storage
depmod -a
```

Espere unos minutos y verifique el mensaje que ha emitido el sistema en el buzón entrada de la cuenta de correo electrónico definida.

87.2.6. Reglas de UDEV para impedir el acceso a unidades de almacenamiento USB.

UDEV es una colección de herramientas y un servicio que se encarga de gestionar los eventos recibidos desde el núcleo del sistema, encargándose de éstos en el espacio de usuario. Se encarga de gestionar los permisos correspondientes, crear y eliminar enlaces simbólicos importantes hacia los nodos de los dispositivos que están dentro del directorio **/dev**, cuando los componentes de *hardware* son descubiertos o removidos del sistema.

87.2.6.1. En CentOS, Fedora, SUSE Linux Enterprise y Red Hat Enterprise Linux.

Para restringir el acceso a las unidades de almacenamiento USB, se debe crear un archivo denominado **/etc/udev/rules.d/10-usb-storage.rules**:

```
vim /etc/udev/rules.d/10-usb-storage.rules
```

Añada el siguiente contenido:

```
DRIVER=="usb-storage", OPTIONS+="ignore_device last_rule"
```

Lo anterior establece que al utilizar el módulo **usb-storage**, se ignoren los dispositivos a los que corresponda y que se impida añadir nuevas reglas que pudieran cambiar esta política.

Para que apliquen los cambios, es necesario reiniciar el sistema.

```
reboot
```

Inserte cualquier unidad de almacenamiento USB para verificar que es imposible acceder hacia el contenido de ésta.

87.2.6.2. En openSUSE.

Para restringir el acceso a las unidades de almacenamiento USB, se debe crear un archivo denominado **/etc/udev/rules.d/10-uas.rules**:

```
vim /etc/udev/rules.d/10-uas.rules
```

Añada el siguiente contenido:

```
DRIVER=="uas", OPTIONS+="ignore_device last_rule"
```

Lo anterior establece que al utilizar el módulo **uas**, se ignoren los dispositivos a los que corresponda y que se impida añadir nuevas reglas que pudieran cambiar esta política.

Para que apliquen los cambios, es necesario reiniciar el sistema.

```
reboot
```

Inserte cualquier unidad de almacenamiento USB para verificar que es imposible acceder hacia el contenido de ésta.

87.2.7. PolicyKit para restringir el acceso a unidades de almacenamiento externo en general.

PolicyKit es un conjunto de herramientas para definir y gestionar la autorización hacia diversas operaciones en el sistema.

87.2.7.1. En CentOS, Fedora, openSUSE y Red Hat Enterprise Linux.

Estos sistemas operativos utilizan PolicyKit 0.94 o versiones más recientes. La configuración varía respecto de las de versiones anteriores.

Lo primero es determinar el estado de la política **org.freedesktop.udisks.filesystem-mount-system-internal**, ejecutando lo siguiente:

```
pkaction --action-id \
    org.freedesktop.udisks.filesystem-mount-system-internal \
    --verbose
```

Para definir la política que sólo permitirá montar unidades de almacenamiento externo (USB, CDROM y DVDROM) al usuario root, se crear el archivo /var/lib/polkit-1/localauthority/50-local.d/udisks.pkla:

```
vim /var/lib/polkit-1/localauthority/50-local.d/udisks.pkla
```

Y se añade el siguiente contenido:

```
[Unidades de almacenamiento]
Identity=unix-user:*
Action=org.freedesktop.udisks.filesystem-mount-system-internal
ResultAny=auth_admin
ResultInactive=auth_admin
ResultActive=auth_admin
```

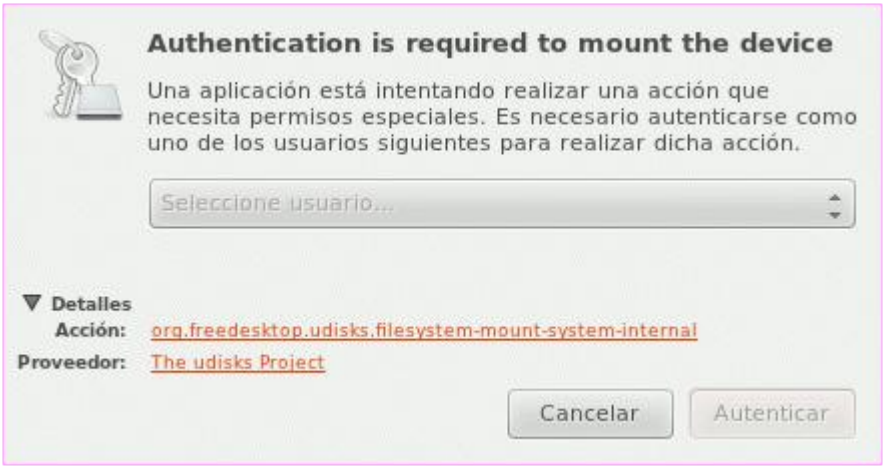
Para permitir sólo a un usuario en particular, se cambia **unix-user:*** (define a cualquier usuario del sistema) por **unix-user:usuario**. En el siguiente ejemplo se permite el uso solo al usuario fulano:

```
[Unidades de almacenamiento]
Identity=unix-user:fulano
Action=org.freedesktop.udisks.filesystem-mount-system-internal
ResultAny=auth_admin
ResultInactive=auth_admin
ResultActive=auth_admin
```

Para verificar lo anterior, se puede ejecutar como root lo siguiente, donde 1586 corresponde al número de identidad de proceso de gnome-session y fulano corresponde al nombre del usuario activo del escritorio:

```
pkcheck --action-id \
    org.freedesktop.udisks.filesystem-mount-system-internal \
    --process 1586 -u fulano
```

Lo anterior debe devolver una ventana de autenticación similar a la siguiente.



Ventana de autenticación para administradores.

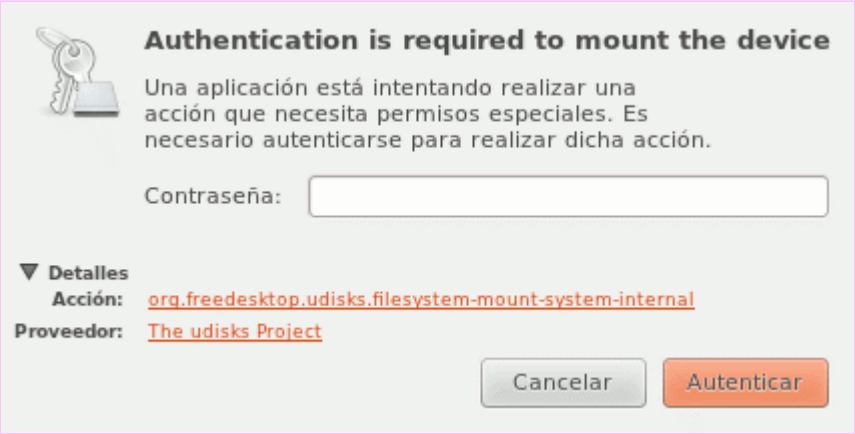
Si se quiere que en el caso anterior se use la contraseña del mismo usuario, para evitar proporcionar la contraseña de root, cambie auth_admin por **auth_self**:

```
[Unidades de almacenamiento]
Identity=unix-user:fulano
Action=org.freedesktop.udisks.filesystem-mount-system-internal
ResultAny=auth_self
ResultInactive=auth_self
ResultActive=auth_self
```

Para verificar lo anterior, se puede ejecutar como root lo siguiente, donde 1586 corresponde al número de identidad de proceso de gnome-session y fulano corresponde al nombre del usuario activo del escritorio:

```
pkcheck --action-id \
    org.freedesktop.udisks.filesystem-mount-system-internal \
    --process 1586 -u fulano
```

Lo anterior debe devolver una ventana de autenticación similar a la siguiente.



Ventana de autenticación para usuario.

Inserte una unidad de almacenamiento USB o disco CD o DVD y verifique que aparece una ventana de autenticación, similar a cualquiera de las de arriba.

Si sólo se desea prohibir el acceso a las unidades de almacenamiento externo a un solo usuario, se cambia **auth_self** por **no**:

```
[Unidades de almacenamiento]
Identity=unix-user:fulano
Action=org.freedesktop.udisks.filesystem-mount-system-internal
ResultAny=no
ResultInactive=no
ResultActive=no
```

Lo anterior impedirá que el usuario fulano pueda hacer uso de unidades de almacenamiento externo por completo, sin mostrar siquiera la ventana de autenticación.

Para eliminar la política, simplemente se elimina el archivo **udisks.pkla**.

```
rm -f /var/lib/polkit-1/localauthority/50-local.d/udisks.pkla
```

87.2.7.2. En SUSE Linux Enterprise 11.

Este sistemas operativo utiliza **PolicyKit 0.90**. La configuración varía respecto de las de versiones posteriores. cabe señalar que SUSE Linux Enterprise 10 carece de soporte para PolicyKit, por lo cual el procedimiento sólo aplica para la versión 11 y posteriores.

Lo primero es determinar el estado de la política **org.freedesktop.hal.storage.mount-removable**, ejecutando lo siguiente:

```
polkit-action --action \
    org.freedesktop.hal.storage.mount-removable
```

Para definir la política que sólo permitirá montar unidades de almacenamiento externo (USB, CDROM y DVDROM) al usuario root, se edita el archivo **/etc/polkit-default-privs.local**:

```
vim /etc/polkit-default-privs.local
```

Y se añade el siguiente contenido:

```
org.freedesktop.hal.storage.mount-removable    auth_admin_keep_always
```

Al terminar se ejecuta el mandato **set_polkit_default_privs** para que se active la política.

```
set_polkit_default_privs
```

Para permitir que sólo un usuario regular en particular pueda hacer uso de las unidades de almacenamiento externo, se ejecuta el mandato **polkit-auth** del siguiente modo:

```
polkit-auth --user fulano --grant \
    org.freedesktop.hal.storage.mount-removable
```

Para deshacer el cambio, se ejecuta lo siguiente:

```
polkit-auth --user fulano --revoke \
    org.freedesktop.hal.storage.mount-removable
```

Para impedir que un solo usuario sea quien tenga prohibido hacer uso de las unidades de almacenamiento externo, se omiten todos los procedimientos anteriores y se ejecuta:

```
polkit-auth --user fulano --block \
    org.freedesktop.hal.storage.mount-removable
```

Para determinar los permisos de acceso de un usuario en particular para org.freedesktop.hal.storage.mount-removable, se ejecuta:

```
polkit-auth --user fulano --explicit \
    org.freedesktop.hal.storage.mount-removable
```

Inserte una unidad de almacenamiento USB o disco CD o DVD y verifique que aparece una ventana de autenticación, similar a las de arriba.

88. Administración de configuraciones de GNOME 2.

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

© 1999-2013 Joel Barrios Dueñas. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. **b) No puede utilizar esta obra para fines comerciales.** c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

88.1. Introducción.

El escritorio de GNOME 2 utiliza GConf para almacenar y administrar la configuración de la mayor parte de sus componentes. Se ejecuta en segundo plano como gconfd-2 e inicia automáticamente junto con el escritorio, sólo una instancia por usuario.

La configuración del escritorio puede hacerse desde las preferencias de las aplicaciones individuales, desde el Centro de Control, utilizando el mandato **gconftool-2** o bien a través de la herramienta gráfica **gconf-editor**.

GConf almacena las configuraciones de los usuarios en el directorio **~/.gconf** de cada usuarios. Los datos dentro de este directorio sólo pueden ser modificados por las preferencias de las aplicaciones y componentes del escritorio, el mandato **gconftool-2** o bien la herramienta gráfica **gconf-editor**. Cualquier modificación realizada con editor de texto dentro de este directorio, será ignorada por completo por gconfd-2 y se perderá irremediablemente al cerrar la sesión.

88.2. Mandato gconftool-2.

El mandato **gconftool-2** puede ser utilizado como usuario regular para cambiar el valor de cualquier configuración almacenada dentro del directorio **~/.gconf**. Como root es posible cambiar los valores predeterminados o bien establecer valores obligatorios.

Para obtener una lista completa de las opciones de configuración del escritorio de un usuario regular, junto con los valores que éstas tengan, se ejecuta el mandato **gconftool-2** con la opción **--recursive-list** (o bien -R) y /desktop/gnome (sin diagonal al final) como argumento:

```
gconftool-2 --recursive-list /desktop/gnome
```

Para obtener una lista completa de las opciones de configuración de las aplicaciones que utilizan GConf, junto con los valores que éstas tengan, como usuario regular, se ejecuta el mandato **gconftool-2** con la opción **--recursive-list** (o bien -R) y /apps (sin diagonal al final) como argumento:

```
gconftool-2 --recursive-list /apps
```

Para realizar la búsqueda de una clave en particular, se ejecuta el mandato **gconftool-2** con la opción **--search-key-regex**, seguida de una expresión regular o cadena de texto que se desee buscar. En el siguiente ejemplo se realiza la búsqueda de claves que coincidan con la cadena *picture_filename*:

```
gconftool-2 --search-key-regex picture_filename
```

Para obtener una descripción corta de una clave en particular, se ejecuta gconftool-2, con la opción **--short-docs** y el nombre de la clave como argumento. En el siguiente ejemplo se consulta la descripción corta de la clave /desktop/gnome/background/picture_filename:

```
gconftool-2 --short-docs \
    /desktop/gnome/background/picture_filename
```

Lo anterior devolverá en esta clave se establece un archivo de imagen.

Para obtener una descripción de una clave en particular, se ejecuta gconftool-2, con la opción **--long-docs** y el nombre de la clave como argumento. En el siguiente ejemplo se consulta la descripción de la clave /desktop/gnome/background/picture_filename:

```
gconftool-2 --long-docs \
    /desktop/gnome/background/picture_filename
```

Lo anterior devolverá que se trata de la configuración para establecer el tapiz o fondo de pantalla del escritorio.

Para obtener los valores de una clave en particular, como usuario regular, se utiliza el mandato **gconftool-2** con la opción **--get** (o bien -g) y el nombre de la clave como argumento. En el siguiente ejemplo se consulta el valor de /desktop/gnome/background/picture_filename, que corresponde al archivo de imagen utilizado como fondo de pantalla del escritorio:

```
gconftool-2 --get /desktop/gnome/background/picture_filename
```

La salida puede devolver algo similar a lo siguiente:

```
/usr/share/backgrounds/waves/waves.xml
```

Para cambiar cambiar el valor de esta configuración, sólo para el usuario regular utilizado, se ejecuta el mandato **gconftool-2** con la opción **--set** (o bien -s), el nombre de la clave, la opción **--type** (o bien -t) y el tipo de valor (bool, float, int, list, pair o string para definir valores tipo booleano, flotante, entero, lista, par o cadena, respectivamente) y finalmente el valor a establecer para la clave. En el siguiente ejemplo se establece /usr/share/backgrounds/cosmos/jupiter.jpg como el valor para la clave /desktop/gnome/background/picture_filename:

```
gconftool-2 --set /desktop/gnome/background/picture_filename \
    --type string "/usr/share/backgrounds/cosmos/jupiter.jpg"
```

Para regresar una clave a su valor predeterminado, se ejecuta el mandato **gconftool-2** con la opción **--unset** (o bien -u) y el nombre de la clave como argumento. En el siguiente ejemplo se elimina el valor personalizado para el clave /desktop/gnome/background/picture_filename:

```
gconftool-2 --unset /desktop/gnome/background/picture_filename
```

Para regresar a sus valores predeterminados varias claves que están dentro un mismo directorio, se ejecuta el mandato **gconftool-2** con la opción --recursive-unset y el nombre del directorio sobre el cual se eliminarán de manera recursiva los valores personalizados. En el siguiente ejemplo, se eliminarán los valores personalizados de todas las configuraciones que están debajo de **/desktop/gnome/background**:

```
gconftool-2 --recursive-unset /desktop/gnome/background
```

Para establecer valores predeterminados, se utiliza gconftool-2 como root, con la opción **--direct** (acceso directo a la base de datos de configuraciones), la opción **--config-source** con la ruta **xml:readwrite:/etc/gconf/gconf.xml.defaults**, la opción **--set** con el nombre de la clave cambiar, la opción **--type** con el tipo de valor y el valor que se desea establecer como predeterminado para una clave en particular. En el siguiente ejemplo se establecerá el archivo **/usr/share/backgrounds/cosmos/jupiter.jpg** como el valor predeterminado de **/desktop/gnome/background/picture_filename**:

```
gconftool-2 --direct \
    --config-source xml:readwrite:/etc/gconf/gconf.xml.defaults \
    --set /desktop/gnome/background/picture_filename \
    --type string "/usr/share/backgrounds/cosmos/jupiter.jpg"
```

Lo anterior hará que cuando el usuario ejecute lo siguiente:

```
gconftool-2 --unset /desktop/gnome/background/picture_filename
```

Se muestre como imagen predeterminada al archivo **/usr/share/backgrounds/cosmos/jupiter.jpg** en la que se estableció originalmente en el sistema. El usuario podrá establecer cualquier otra imagen que desee como fondo de escritorio y cuando elimine su configuración personalizada para esta clave, se mostrará la imagen que se haya establecido como predeterminada.

Para regresar una clave al valor original, se ejecuta el mandato **gconftool-2** con la opción **--direct**, la opción **--config-source** con la ruta **xml:readwrite:/etc/gconf/gconf.xml.defaults** y la opción **--unset**. En el siguiente ejemplo se regresará a su valor original la clave /desktop/gnome/background/picture_filename:

```
gconftool-2 --direct \
    --config-source xml:readwrite:/etc/gconf/gconf.xml.defaults \
    --unset /desktop/gnome/background/picture_filename
```

Para establecer valores obligatorios, es decir configuraciones que los usuarios estarán imposibilitados para cambiar, se utiliza gconftool-2 como root, con la opción **--direct** (acceso directo a la base de datos de configuraciones), la opción **--config-source** con la ruta **xml:readwrite:/etc/gconf/gconf.xml.mandatory**, la opción **--set** con el nombre de la clave a cambiar, la opción **--type** con el tipo de valor y el valor que se desea establecer como predeterminado para una clave en particular. En el siguiente ejemplo se establecerá /usr/share/backgrounds/cosmos/jupiter.jpg como el valor obligatorio de /desktop/gnome/background/picture_filename:

```
gconftool-2 --direct \
    --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory \
    --set /desktop/gnome/background/picture_filename \
    --type string "/usr/share/backgrounds/cosmos/jupiter.jpg"
```

Para poder apreciar este cambio en particular, es necesario cerrar la sesión de escritorio que esté activo y volver a ingresar a éste. En algunos casos sólo será necesario cerrar y volver a ejecutar una aplicación en particular para la cual se hayan establecido los valores obligatorios.

Para regresar una clave al valor original, se ejecuta el mandato **gconftool-2** con la opción **--direct**, la opción **--config-source** con la ruta **xml:readwrite:/etc/gconf/gconf.xml.defaults** y la opción **--unset**. En el siguiente ejemplo se regresará a su valor original la clave /desktop/gnome/background/picture_filename:

```
gconftool-2 --direct \
    --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory \
    --unset /desktop/gnome/background/picture_filename
```

La mayoría de las distribuciones actuales de GNU/Linux utilizan las rutas **/etc/gconf/gconf.xml.defaults** y **/etc/gconf/gconf.xml.mandatory**, por lo cual todo lo anterior deberá funcionar sin problemas. En SUSE Linux Enterprise 10 y versiones anteriores, las rutas son **/etc/opt/gnome/gconf/gconf.xml.defaults** y **/etc/opt/gnome/gconf/gconf.xml.mandatory**, para las configuraciones predeterminadas y obligatorias, respectivamente.

88.2.1. Configuraciones más comúnmente restringidas en el escritorio de GNOME.

- **/desktop/gnome/lockdown/disable_application_handlers**:
  Tipo de valor booleano. Si se establece el valor true, prevenir que cualquier aplicación ejecute cualquier gestor de URL o tipos MIME.

- **/desktop/gnome/lockdown/disable_command_line**:
  Tipo de valor booleano. Si se establece el valor true, impide que el usuario acceda a la terminal de GNOME o que especifique una línea de mandatos para ser ejecutada. Esto también desactiva el acceso al diálogo del panel «Ejecutar aplicación».

- **/desktop/gnome/lockdown/disable_lock_screen**:
  Tipo de valor booleano. Si se establece el valor true, previene que el usuario bloquee su pantalla.

- **/desktop/gnome/lockdown/disable_printing**:
  Tipo de valor booleano. Si se establece el valor true, impide que el usuario imprima. Desactiva el acceso a todos los diálogos «Imprimir» de todas las aplicaciones para GNOME.

- **/desktop/gnome/lockdown/disable_print_setup**:
  Tipo de valor booleano. Si se establece el valor true, impide que el usuario pueda modificar los ajustes de impresión. Desactiva el acceso a todos los diálogos «Configurar impresión» de todas las aplicaciones.

- **/desktop/gnome/lockdown/disable_save_to_disk**:
  Tipo de valor booleano. Si se establece el valor true, impide que el usuario pueda guardar archivos en el disco. Desactiva el acceso a todos los diálogos «Guardar como» de todas las aplicaciones.

- **/desktop/gnome/lockdown/disable_user_switching**:
  Tipo de valor booleano. Si se establece el valor true, previene que el usuario seleccione otra cuenta mientras su sesión está activa.

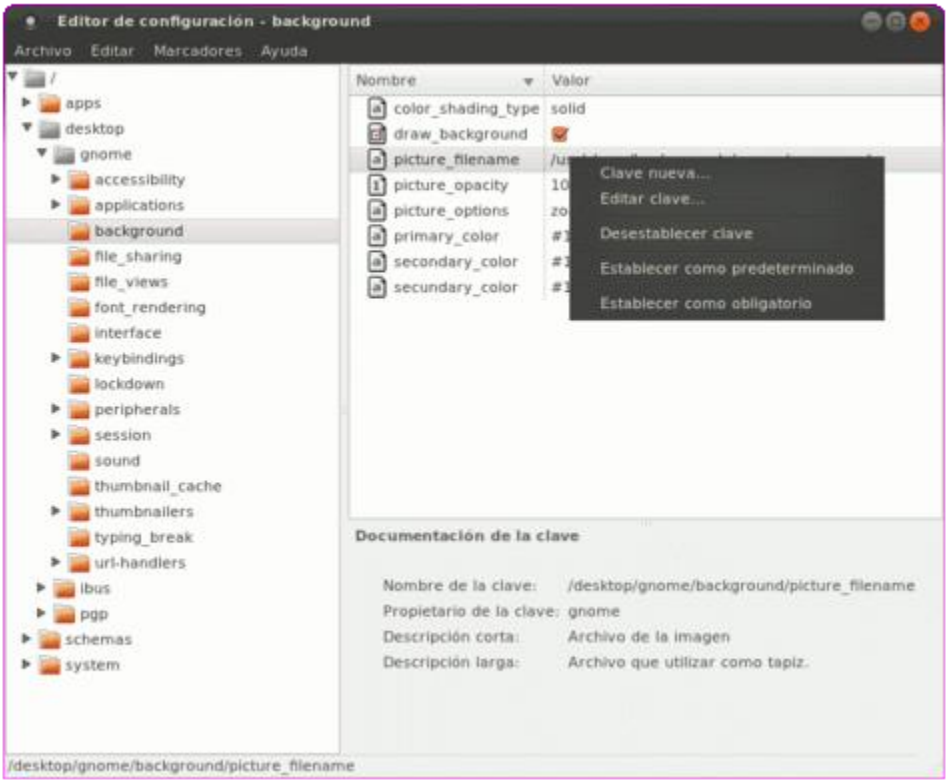
- **/apps/nautilus/lockdown/disable_context_menus**:
  Tipo de valor booleano. Si se establece el valor true, previene que los usuarios puedan utilizar los menúes contextuales del administrador de archivos. Muy recomendado para kioskos.

- **/apps/panel/global/disable_log_out**:
  Tipo de valor booleano. Si se establece el valor true, el panel impedirá al usuario cerrar la sesión, eliminando las entradas de menú de salida de sesión.

- **/apps/panel/global/locked_down**:
  Tipo de valor booleano. Si se establece el valor true, el panel impedirá cambios en su configuración. Algunas mini-aplicaciones individuales quizá necesiten bloquearse de forma independiente. El panel (o la sesión) debe reiniciarse para que esto surta efecto.

Herramienta gconf-editor.

La herramienta gráfica **gconf-editor** permite hacer todo lo que hace gconftool-2, pero con una interfaz gráfica. Sólo es necesario localizar y seleccionar la clave, hacer clic derecho y editar el valor de la clave o bien desestablecer ésta o bien establecer el valor de la clave como predeterminado u obligatorio. Para distribuciones que incluyen PolicyKit (o polkit), aparecerá un diálogo que solicitará la contraseña del administrador cuando se requiera establecer valores predeterminados u obligatorios. Para las distribuciones que carecen de PolicyKit, es necesario ejecutar gconf-editor como root a fin de poder establecer valores predeterminados u obligatorios.



GConf-editor.

En caso de ser necesario, puede instalarse en CentOS, Fedora y Red Hat Enterprise Linux ejecutando:

```
yum -y install gconf-editor
```

En caso de ser necesario, puede instalarse en openSUSE y SUSE Linux Enterprise ejecutando:

```
yast -i gconf-editor
```

Notas

Notas

Notas

Notas